



A ALMENARA

REGIMENTO DE TRANSMISSÕES

ANO V - Nº 05 - 2013

A Informação na palma das mãos ...





BRASÃO DE ARMAS DO REGIMENTO DE TRANSMISSÕES

Descrição Heráldica:

- Escudo de azul, uma almenara de ouro, iluminada e aberta de vermelho e acesa do mesmo perfilado de ouro;
- Elmo militar, de prata, forrado de vermelho, a três quartos para a dextra;
- Correia de vermelho, perfilada de ouro;
- Paquife e virol de azul e ouro;
- Timbre: uma garra de leão de vermelho empunhando seis raios eléctricos de ouro;
- Divisa: num listel branco, ondulado, sotoposto ao escudo, em letras de negro, maiúsculas, estilo elzevir «SEMPRE MELHOR».

Simbologia e Alusões das Peças:

- A ALMENARA (torre de sinais) é símbolo heráldico das comunicações.

Representação e Significado dos Metais e Cobres:

- Ouro: sol, nobreza;
- VERMELHO: fogo, energia criadora;
- AZUL: ar, espaço, lealdade.

Sumário

Descrição Heráldica do Regimento de Transmissões.....	2
Editorial.....	4
Coleção visitável do Regimento de Transmissões.....	6
Sistemas Integrados de Serviços Digitais.....	14
O SharePoint como uma plataforma de desenvolvimento para o Portal de Lições Aprendidas	22
Sistema de Videoconferência do Exército.....	28
Protocolo de Autenticação na Web - OpenID	30
A Segurança de Informação e a Gestão de Eventos.....	34
Contributo da Análise Forense Digital para a capacidade de <i>Intelligence</i> do Exército.....	40
Enquadramento Estratégico e Fundamentos para o desenvolvimento da Capacidade Nacional de Ciberdefesa	48
The National Cybersecurity Workforce Framework - USA / EUA.....	52
Comunicações HF Com Antenas NVIS	56
SITEP – Fibra Ótica	60
Viaturas Automóveis de Projetores.....	66
A contribuição das U/E/O do Exército para o Programa ECO.AP.....	70
Resumo de Atividades	74
Galeria de Comandantes	86
Sinopse Histórica	94

EDITORIAL

O Regimento de Transmissões (RT) comemora os seus 36 anos de existência. Criado em 1977 no Aquartelamento da Cruz dos Quatro Caminhos em Lisboa, herdou na sua génese a história e a missão do Serviço de Telecomunicações Permanentes (STM). É longa a história deste aquartelamento ao serviço das Transmissões, cujas referências mais remotas a unidades constituídas neste local, reportam ao Batalhão de Telegrafistas, criado em 1937. Recuando no tempo, a história deste aquartelamento ao serviço das Transmissões, inicia-se com a inauguração da primeira Rede Telegráfica do Exército, no dia 17 de Setembro de 1873, com instalação neste local de uma das 13 estações que constituíam essa rede. Desde então, as transformações foram inúmeras, ao ritmo da evolução tecnológica. As últimas transformações ocorreram com a incorporação no RT, em 2005, de valências de Segurança das comunicações, até então residentes no BISM. Posteriormente, em 2007, com a transferência de valências do CIE e em 2009, com a criação do Elemento de Guerra de Informação e da estrutura CIRC do Exército.



Atualmente damos continuidade à história quase bicentenária desta unidade, através de um novo processo de mudança, que acompanha a reestruturação em curso no Exército. Neste processo, colocam-se-nos vários desafios. Em primeiro lugar, o desafio da eficiência. Este é um objetivo sempre presente nas organizações, mas que no atual contexto económico do País, torna-se um desígnio obrigatório para o Exército em geral, e para esta unidade em particular. No âmbito interno às Transmissões, a criação da Escola das Armas, constitui mais um polo no Exército que requer a afetação de quadros de Tm, o que dificultará a concentração de recursos humanos nesta unidade. O Exército continua a necessitar de um adequado apoio de Comunicações e Sistemas de Informação, a operacionalizar através desta unidade, no âmbito do SIC-Op. A manutenção desta missão, sem comprometer a qualidade dos serviços e num contexto de recursos humanos mais limitados, só será possível cumprindo com próprio lema da unidade “SEMPRE MELHOR”, que nos apela a fazer mais e melhor com os mesmos recursos. Ainda na senda da almejada eficiência, não podemos descurar o contributo essencial dos sistemas de Informação para a eficiência geral do Exército. O desenvolvimento adequado destes sistemas, potenciará a redução de recursos humanos afetos às atividades de gestão e até de apoio à decisão, de que o desenvolvimento do conceito “*Business Intelligence*” é um bom exemplo.

Em segundo lugar, o desafio da melhor resposta à “revolução” tecnológica e ao impacto que esta tem na área das Transmissões. É hoje claro que a “revolução” tecnológica iniciada com o aparecimento das redes de computadores, que conduziu à hiper-conetividade que caracteriza a sociedade da informação, é também uma realidade ao nível do ambiente tecnológico em que as Forças Armadas terão que desenvolver a sua atividade. A missão principal das Transmissões, há muito tempo deixou de ser a entrega da mensagem ou o estabelecimento da comunicação, nem tão pouco são os sistemas de informação! O desafio atual está recentrado na INFORMAÇÃO, que adquiriu estatuto de recurso de elevado valor, cuja superioridade em contexto operacional, é necessário assegurar. Por outro lado, a emergência do Ciberespaço como nova dimensão do campo de batalha é uma realidade já assumida ao nível dos conceitos doutrinários. Este espaço, de limites indefinidos e de utilização obrigatória em qualquer contexto operacional, constitui um novo domínio de confronto que os Exércitos modernos não poderão descurar e que deverá ter impacto no desenvolvimento de capacidades operacionais. A Segurança da Informação e o Comando e Controlo, passaram a depender da capacidade de compreender e controlar todos os elementos que interagem neste espaço, através de uma eficaz capacidade de Cibersegurança, que assegure a proteção das infraestruturas críticas de CIS contra Ciberataques. Por outro lado, a exploração operacional deste novo domínio, através da

condução de “*Computer Network Operations*”, exige o desenvolvimento de uma capacidade de Ciberdefesa, capacidade a desenvolver num quadro conjunto e cooperativo, e para o qual esta unidade muito poderá contribuir.

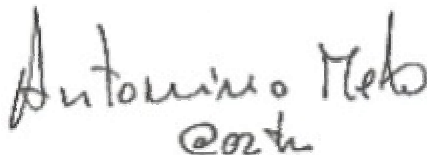
O momento atual tem a particularidade de marcar um novo ciclo na vida desta unidade. A transformação em curso no Exército conceptualiza as unidades Regimentais como geradoras de Elementos da Componente Operacional do Sistema de Forças do Exército, e nessa conformidade, a estrutura Regimental desta unidade será deslocalizada para o Porto, para a atual Escola Prática de Transmissões, que será extinta, assumindo a natureza Regimental, ao serviço das Transmissões de Campanha e, cumulativamente, constitui um polo de formação técnica na área de Transmissões. No aquartelamento da Cruz dos Quatro Caminhos, continuam as atuais valências operacionais, integradas na Direção de Comunicações e Sistemas de Informação. Manter-se-á assim uma continuidade histórica da missão desta unidade no apoio de Transmissões à estrutura Permanente do Exército, que se verifica desde 1951, com a criação do então Serviço de Telecomunicações Permanentes.

O número da Revista Almenara, agora publicado, espelha na perfeição a história secular desta unidade ao serviço das Transmissões. A inclusão de artigos de antigos oficiais de Transmissões, como o Tenente coronel Rodrigo Leitão que partilha a sua experiência com a utilização de antenas NVIS no Ultramar e o Coronel Cruz Fernandes, com um artigo sobre Fibras Óticas, evidenciam também o forte espírito de pertença e de ligação às Transmissões e a esta unidade que transcende o tempo de prestação de serviço efetivo, o que a todos nos orgulha e motiva.

Contamos também com o contributo da Comissão da História das Transmissões, que reflete o muito trabalho e atividade desenvolvido por esta comissão durante o último ano. A preparação da coleção visitável das Transmissões constituía um objetivo de longa data, tendo sido possível, com um esforço notável dos seus membros, preparar os equipamentos e o espaço que doravante constituirá certamente um cartão-de-visita desta unidade. Estou certo de interpretar o sentir de todos os militares ao expressar o mais profundo reconhecimento aos ilustres camaradas desta comissão, pelo seu contributo abnegado na preservação deste legado histórico, perpetuando no tempo as referências a um passado, de que muito nos orgulhamos e de que pretendemos ser dignos continuadores.

A todos os que colaboraram com a elaboração de artigos expresso os mais sinceros agradecimentos pelo prestimoso contributo para a afirmação das Transmissões e desta unidade, como um importante pilar do Exército. Agradeço igualmente a todos os profissionais que servem no Regimento de Transmissões e que nas diversas áreas demonstraram extrema dedicação, competência e profissionalismo, dando continuidade à história centenária do Quartel dos Quatro Caminhos ao serviço das Transmissões Permanentes, e o garante de que continuaremos a fazer **“SEMPRE MELHOR”**.

O Comandante do RT

A handwritten signature in dark ink, reading "Antonino Melo" with a stylized flourish underneath.

Antonino Melchior Pereira de Melo
Cor Tm (Eng)



História

Coleção visitável do Regimento de Transmissões

No dia 20 de setembro de 2013 será reaberta a Coleção Visitável do Regimento de Transmissões cumprindo a vontade do seu atual comandante, coronel Tm (Eng) Antonino Melo.

A reabertura corresponde a uma primeira fase do que se pretende que venha a ser a Coleção Visitável. A apresentação tem falta de alguns elementos de contextualização dos vários períodos da história da Unidade, que se prevê completar durante o próximo ano.

A Coleção Visitável (assim como o Polo Museológico de Transmissões do Museu Militar de Elvas) tem origem no anterior Museu de Transmissões e dá cumprimento ao despacho nº 96/CEME/08, NORMAS GERAIS DOS MUSEUS E COLECÇÕES VISITÁVEIS DO EXÉRCITO.

“A Coleção Visitável destina-se a apresentar a evolução das Transmissões de que foi testemunha o Regimento de Transmissões, e todas as Unidades que o antecederam, e de quem foram herdeiras, desde 1810 até à atualidade...”



A novidade desta nova reorganização consiste no facto de, como Coleção Visitável, se procurar expor material de Transmissões ligado à memória das várias unidades de Transmissões que tiveram a sua sede no Quartel de Sapadores, incluindo aquelas de que se tornaram herdeiras, deixando para o Museu de Elvas a representação de toda a História das Transmissões Militares.

Antecedentes

Data de 1971 a primeira iniciativa de carácter museológico na área das Transmissões protagonizada pelo brigadeiro Machado de Sousa, então Diretor da Arma, que tomou a iniciativa de expor nas instalações da Direção, no Campo de Santa Clara, uma coleção de material de Transmissões antigo, que vinha sendo recolhido e classificado.

Nos anos seguintes o coronel Engº Guilherme Bastos Moreira, através de persistente recolha de equipamentos nas unidades do país, que a sua função de Inspetor facilitava, aumentou consideravelmente a coleção. Ele próprio elaborou um estudo para a instalação da coleção no Regimento de Transmissões, dada a falta de espaço com que se deparou, que veio a conjugar-se com outro estudo efetuado pelo capitão Engº Tm Carlos Rosado.



O apoio financeiro da Direção Geral de Instrução, então encabeçada pelo general Altino de Magalhães, tornou possível a concretização das obras necessárias, sendo Diretor da Arma o brigadeiro Pereira Pinto e Comandante do Regimento de Transmissões o coronel Engº Pedroso de Lima. O projeto coube à arquiteta Teresa Almendra que contou com a colaboração do Coronel Engº José Maria Marques (pintor José de Guimarães).

Em 31 de março de 1978 foi inaugurado finalmente o Museu, tendo presidido à cerimónia o Vice-Chefe do Estado-Maior do Exército, general Melo Egídio, passando o Coronel Engº Guilherme Bastos Moreira a exercer o cargo de Diretor.



Museu de Transmissões do Regimento de Transmissões

No final do ano de 1980 e início de 1981 foram abertas mais duas salas ao público, por iniciativa do comandante do Regimento, coronel Engº Araújo Gerales, com a colaboração do coronel Engº Pinto dos Santos, tenente-coronel Engº Tm Figueira, coronel Engº Rego Falcão e tenente-coronel Engº Tm Campos Soares.

Em 1984, o comandante do Regimento de Transmissões, coronel Engº Tm Cruz Fernandes, empenhou-se pessoalmente no projeto de remodelação do Museu, de que resultaram modificações estruturais significativas.

Em 1990, comandando o Regimento de Transmissões o coronel Engº Tm Maia de Freitas, a área de exposição foi aumentada com mais duas salas.

A obra do coronel Engº Guilherme Bastos Moreira como Diretor foi um exemplo de notável dedicação à Arma, que se traduziu, não só na valiosa coleção que nos deixou e sempre procurou valorizar, mas também na publicação das suas “Notas sobre as Transmissões Militares”, livro de referência na historiografia militar na área das Transmissões.



Coronel Engº Guilherme Bastos Moreira

O desaparecimento do coronel Engº Guilherme Bastos Moreira, em 2002, pela dificuldade da sua substituição, pôs em causa a própria continuidade do Museu, tendo-se admitido como inevitável a sua extinção, o que foi superado pelo comandante do Regimento de Transmissões, coronel Tm (Engº) Edorindo Ferreira, que conseguiu a reabertura do Museu em 2003, através da formação do Grupo dos Amigos do Museu, constituído por oficiais e sargentos de Transmissões, na situação de reserva ou reforma, nomeadamente: major-general Pedroso de Lima, major-general Pinto Castro, coronel Engº Tm Costa Dias, tenente-coronel Engº Tm Jorge Golias e sargentos-mores Leal, Florindo (já falecido) e Barroso.



Sala de exposição do Museu de Transmissões

Em setembro de 2005, sob o comando do coronel Engº Tm Henriques Dinis, integrado nas comemorações do Dia do Regimento de



Transmissões, inaugurou-se a “Sala DGMT”, onde se pretendeu preservar a memória histórica do Depósito Geral de Material de Transmissões, singular órgão logístico da Arma de Transmissões, extinto em dezembro de 2002. O espólio desta sala irá brevemente ser exposto no Museu Militar de Elvas.

A partir de 2008 o Museu tem estado fechado ao público, em virtude do apoio que o Exército passou a dar à Fundação Portuguesa das Comunicações na realização de uma exposição de material militar de Transmissões dos três ramos das Forças Armadas, que se realizou na sede daquela Fundação. Tratou-se de uma exposição de vulto, que esteve aberta ao público durante quase um ano, e na qual o Grupo dos Amigos do Museu, o Regimento de Transmissões e a Escola Prática de Transmissões muito se empenharam, sendo que a maior parte do material exposto pertencia ao Museu das Transmissões.



Cartaz alusivo à exposição Telecomunicações Militares

A abertura da Coleção Visitável esteve prevista para setembro de 2012, mas só agora isso se tornou possível, devendo destacar-se a colaboração da Comissão da História das Transmissões Militares, com a qual o Grupo dos Amigos do Museu se fundiu.

Organização da Coleção Visitável

A Coleção Visitável destina-se a apresentar a evolução das Transmissões de que foi testemunha o Regimento de Transmissões, e todas as Unidades que o antecederam, e das quais foram herdeiras, desde 1810 até à atualidade.

Ao longo dos últimos dois séculos, a evolução tecnológica que permitiu passar das comunicações visuais para as comunicações digitais via satélite, foi sempre no sentido de conseguir comunicações mais rápidas, fiáveis e seguras, mantendo a sobreposição das diversas tecnologias desenvolvidas.

Para enquadramento da apresentação da evolução tecnológica verificada nestes dois séculos foram considerados, os seguintes períodos:

Módulo 1 - O Corpo Telegráfico (1810 – 1864)

Módulo 2 - A sobreposição de meios (1873 – 1900)

Módulo 3 - A liderança da Engenharia (1900 – 1951)

Módulo 4 - O Serviço de Telecomunicações Militares (1951 – 1977)

Módulo 5 - O Regimento de Transmissões (1977 –...)

Módulo 1

O primeiro módulo da Coleção Visitável é dedicado ao Corpo Telegráfico, pioneiro das telecomunicações militares e civis em Portugal. Foi criado em 1810, por iniciativa de D. João VI, tornando-se a primeira unidade de Transmissões.

O Corpo Telegráfico introduziu e operou, no país, dois sistemas que revolucionaram as telecomunicações da época em Portugal.



Modelo do telégrafo de postes

A **telegrafia ótica**, a qual funcionou com base no sistema português inventado por Francisco António Ciera, que já fora utilizado da Guerra Peninsular, que



continuou durante a Guerra (aqui paralelamente ao sistema inglês), prosseguiu nas Lutas Liberais, e acabou por se prolongar até 1855 na rede nacional, altura em que foi substituído pela telegrafia elétrica.

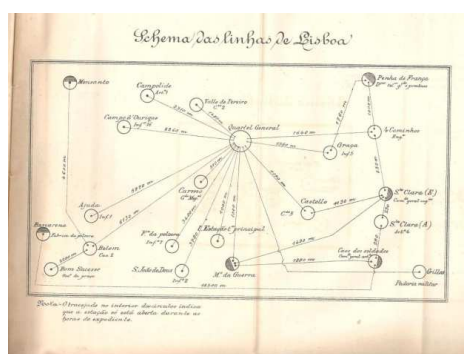
A **telegrafia elétrica**, que foi operada pelo Corpo Telegráfico durante nove anos e posta ao serviço do público nacional e internacional. Era mais rápida e permitia serviço de noite e de dia, independentemente das condições de visibilidade.

Em 1864 o Corpo Telegráfico foi extinto. O seu pessoal foi integrado numa organização civil do Ministério das Obras Públicas, precursora dos CTT.

Módulo 2

O Módulo 2 da Coleção Visitável é dedicado ao período de 1873 a 1900, começando com a inauguração da primeira rede de telegrafia elétrica privativa do Exército em Lisboa, controlada por uma Direção, dependente do Ministro da Guerra.

A estratégia para a reintrodução das Transmissões no Exército deveu-se a Fontes Pereira de Melo e traduziu-se na criação da 1ª rede telegráfica militar em 17 de setembro de 1873 (dia do Regimento de Transmissões) e na criação em 1884 da Companhia de Telegrafistas do Regimento de Engenharia.



Esquema da rede telegráfica militar de Lisboa

A figura dominante deste período foi um oficial de Infantaria, Bon de Sousa que dirigiu o Serviço durante 21 anos (desde o posto de major ao de general de brigada reformado) e que promoveu, com o apoio dos Telégrafos do Reino, a expansão da rede

telegráfica militar por todo o país e a afirmação das Transmissões Permanentes.

O seu esforço levou à “ressurreição” das Transmissões no Exército através da criação duma rede telegráfica militar permanente, constituída pela rede geral e pelas redes especiais de Lisboa e Porto. A rede geral era constituída por estações militares ligadas às estações civis da mesma localidade, permitindo que os despachos chegados à estação civil fossem transmitidos telegraficamente para a estação militar.



Telégrafo impressor de Hughes

Por essa altura o sargento Martins inventou um heliógrafo de que se fabricaram dois modelos: um maior para as transmissões de guarnição e outro mais pequeno para a campanha, tendo sido feitas as primeiras experiências com telefones.

Mas a ação mais inovadora de Bon de Sousa foi a introdução nas Transmissões Permanentes de meios de campanha, dentro do princípio da sobreposição de meios, praticado nos exércitos da época, conjugando o conceito de que as tropas das Transmissões Permanentes deviam estar prontas e treinadas para serem as primeiras a atuar em caso de conflito. Em consequência experimentaram-se novos meios, como os pombos-correios, telefones, semáforos utilizando o código Morse, heliógrafos e lanternas de sinais para serviço noturno.

Módulo 3

O Módulo 3 da Coleção Visitável é dedicado ao período de 1900 a 1951, correspondente à atribuição à Arma de Engenharia da responsabilidade pelas Transmissões Permanentes.



Em 1901 o Serviço Telegráfico Militar passa para a Arma de Engenharia, ficando esta com a responsabilidade completa pelas Transmissões do Exército. Foi nesta altura criada a Companhia de Telegrafistas de Praça, que congregava o pessoal em serviço nas estações das unidades e que teve um papel relevante na Primeira Guerra Mundial.

Nesse ano, o capitão Severo da Cunha fez as primeiras experiências em Portugal com equipamentos rádio (**de faísca**), na parada do Quartel que é hoje a sede do Regimento de Transmissões.

Em 1904 foi instalada a primeira **rede telefónica** militar em Lisboa, com 27 correspondentes, utilizando equipamento sueco da marca Ericsson.

Em 1909 adquiriram-se as primeiras estações de rádio Telefunken para o Exército, que eram transportadas em três viaturas de duas rodas, a cujos varais se atrelava um muar.

A participação na Grande Guerra em França, permitiu que Portugal adotasse o sistema inglês de campanha. O grande vulto desta época foi o Capitão Soares Branco que chefiou o Serviço Telegráfico do Corpo Expedicionário Português, considerado pelo general Comandante como “o que melhor funcionou no CEP”.

A guerra introduziu inovações entre as quais se destacam o “*power buzzer*” que permitia a telegrafia pelo solo (TPS), o *fullerfone*, e o rádio de trincheira a válvulas.

Em 1915, em plena guerra, foi adquirido equipamento rádio Marconi a fim de dotar as unidades que seguiram para África.

Em 1919, com recurso ao material rádio existente, a que se juntou aquele que regressou de França e de África, foi instalada uma **rede radiotelegráfica** cobrindo o País, que serviu em situações de greve ou de alteração de ordem pública.



Equipamento rádio SIF

Em 1926 foi proibida internacionalmente a utilização de rádios de faísca, o que obrigou à aquisição de postos de **onda contínua** para telegrafia e telefonia, da marca SIF (*Société Independente Française de TSF*) e à adaptação, nas oficinas do Regimento de Telegrafistas, dos postos de faísca a postos de onda contínua, numa excecional ação dos seus militares. Iniciou-se a produção de equipamentos rádio para grafia e fonia de 200, 500 e 1000 W, nas oficinas da unidade.

Em 1929 foi adquirido um pequeno lote de estações Marconi de Campanha que foram bastante empregadas no serviço fixo permanente.

Em 1939 iniciou-se a instalação da rede de cabos telefónicos de Lisboa, a fim de substituir a rede filar aérea.

Durante o período da II Guerra Mundial, em que Portugal manteve a neutralidade, foram adquiridos equipamentos P-9, P-11, P-17, P-19, P-21, P-22, P-38, P-58, P-ZC1, SR-HQ, SR-OS, R-103, R-107.

Deve destacar o esforço feito pelas Oficinas Gerais de Material de Engenharia no fabrico de equipamentos sobretudo telefones e centrais telefónicas, durante as décadas de 30 e 40 do século XX, e a construção de redes telefónicas militares nas principais cidades do país.

Neste período, embora se tivesse continuado a seguir a política anterior de sobreposição de meios, tiveram particular relevo a expansão do telefone e do rádio, e a extinção das comunicações heliográficas.



Módulo 4

O Módulo 4 da Coleção Visitável é dedicado ao período de 1951 a 1977, em que o Batalhão de Telegrafistas assumiu o Serviço de Telecomunicações Permanentes (STM). Este Serviço foi criado em 1951, como sucessor do Serviço Telegráfico Militar, tendo o seu controlo passado para o Ministério do Exército, o que originou um considerável salto qualitativo nas comunicações no Continente, Ilhas e Ultramar.

Neste período são de destacar a automatização das redes telefónicas, a introdução dos teleimpressores e respetivas centrais, a introdução de equipamentos de feixes hertzianos, de equipamentos de *fac-símile* e telefotografia e a cobertura radiotelegráfica e telefónica do Continente, Ilhas e Ultramar.

Em 1956 foram instalados em Lisboa os primeiros 12 terminais telegráficos equipados com teleimpressores (T-37 da Siemens) e em 1957 foi instalada uma central manual Siemens de teleimpressores para 20 direções. Na década de 60 foram adquiridos, numa primeira fase, 30 teleimpressores tipo CA, marca Olivetti, e depois 25 da marca Sagem, 30 da marca Siemens T-100 e alguns Olivetti T-315.

A preparação e montagem do Sistema de Transmissões Permanentes de apoio à Guerra Colonial, iniciada em 1958, com antecipação em relação ao início das hostilidades em cada um dos teatros, revelou-se de importância crucial. Nesta ação deve destacar-se a figura do coronel Eng^o Mário Leitão.

Em 1961 iniciaram-se vários trabalhos, como o enterramento em “*duc-tub*” dos novos traçados da Rede Telefónica de Lisboa, as obras para instalação do Centro Emissor Ultramarino (CEU) na Encarnação (Lisboa) e a concretização da rede de feixes hertzianos Lisboa-Santarém-Tomar-Lousã-Aveiro-Porto. Esta rede iniciou-se com a instalação de equipamentos ATE – 800 (VHF) de cinco canais; neste período também se utilizaram equipamentos Marelli (SHF) com 12 canais e Cossor (UHF) de cinco canais.

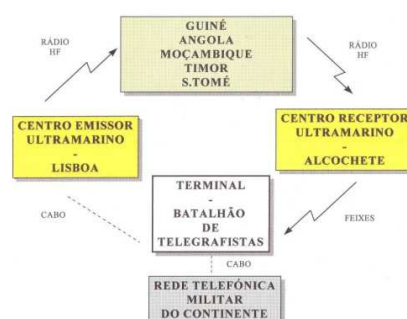
No início de 70 introduziram-se equipamentos GTE – CTR-299 (UHF) de 12 canais.

Em 1962 foi automatizada a rede telefónica de Lisboa, com uma central Strowger de 400 direções, foi instalado o Centro Recetor Ultramarino (CRU) em Alcochete (Campo de Tiro) e respetiva ligação por feixes hertzianos a Lisboa (Centro Nacional de Transmissões, no quartel de Sapadores), e foram estabelecidas as ligações rádio com a Guiné e Cabo Verde.

Em 1963 estabeleceram-se as primeiras ligações Lisboa–Porto, por *fac-símile* e telefotografia, assim como as ligações radiotelegráficas com Angola e Moçambique.

Em 1964 foi substituída a central manual de teleimpressores por uma central automática para 30/40 linhas, concebida pela Automática Elétrica Portuguesa.

Neste período foi criado o Serviço de Som e deram-se os primeiros passos na Guerra Eletrónica.



Esquema de ligações radiotelegráficas com o Ultramar

Todos estes desenvolvimentos permitiram ao Serviço de Telecomunicações Militares instalar, explorar e manter o sistema de transmissões permanente de apoio à Guerra Colonial, compreendendo a montagem rápida de infraestruturas no Continente e em cada um dos Teatros de Operações, o que representou um significativo salto qualitativo e que muito contribuiu para a atuação decisiva das Transmissões no 25 de Abril de 1974.



De facto, a participação do Serviço de Telecomunicações Militares, inserido na Escola Prática de Transmissões, na preparação e execução do golpe militar do 25 de Abril, foi muito importante para o seu êxito. Os sistemas montados acabaram por permitir o apoio eficaz de transmissões às operações e, posteriormente na transmissão e escrutínio dos votos de várias eleições que se seguiram.

Em 1976 foi instalado um sistema de comutação telegráfica, Siemens TDKN.

Módulo 5

Em 1977 o Regimento de Transmissões foi instalado no quartel de Sapadores, sendo a Escola Prática de Transmissões transferida para o Porto. O novo Regimento ficou com parte das atribuições que estavam consignadas ao Serviço de Telecomunicações Militares substituindo-o.

Neste período, com a independência dos territórios ultramarinos, as Transmissões Permanentes reduziram os seus dispositivos às diversas redes do Continente e Ilhas.

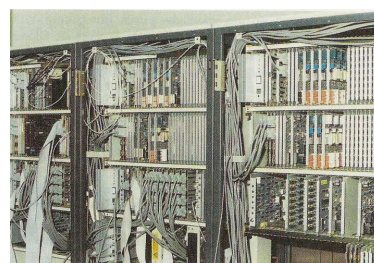
Em 1979 nas redes de feixes hertzianos começou a utilizar material transistorizado da marca FARINON (UHF), de 60 canais

Em 1987 foi feita a instalação de um sistema de comutação automática de mensagens, designado por CROSSROADS, cujos terminais eram teleimpressores Siemens T-1000 e Sagem.

De 1977 a 1981 continuou a fazer-se a automatização telefónica das redes das unidades e redes urbanas e criou-se uma Rede Telefónica Nacional (automática) onde se integraram as Redes Telefónicas de Lisboa, Porto, Coimbra, Elvas, Santa Margarida, Entroncamento, Tancos, Abrantes, Santarém e Caldas da Rainha.

Em 1980, no Porto, retiraram-se os últimos traçados aéreos.

A partir de 1985 começou a desenhar-se um enorme salto qualitativo no Regimento de Transmissões. O seu grande impulsionador foi o coronel Eng^o Tm Cruz Fernandes, “pai” do Sistema Integrado de Telecomunicações do Exército Português (SITEP), fazendo a transição do sistema analógico para o digital. Nesse ano foram adquiridas à firma Centrel Comercial, SA, duas centrais de comutação de voz e dados, da marca OMNI, que entraram em funcionamento a 24 de março de 1987, uma no Regimento de Transmissões e outra no Estado-Maior do Exército. Estas centrais eram de fabrico da empresa belga GTE-ATEA e já então eram utilizadas pela NATO.



Central de comutação de voz e dados, da marca OMNI

Ainda em 1986, o Regimento efetuou o primeiro lançamento de cabo de fibra ótica em Portugal entre o CINCIBERLANT (Comando NATO em Oeiras) e a Escola Militar de Eletromecânica, em Oeiras. A primeira fibra ótica produzida por uma firma Portuguesa (CEL CAT), foi instalada no início de 1987, entre o Regimento de Transmissões e o Estado-Maior do Exército, interligando as duas centrais digitais, com recurso a um inovador equipamento de soldadura de fibra ótica.

Integrado na mesma empreitada foi instalado um moderno sistema de comutação automática de mensagens, designado por CROSSROADS, cujos terminais eram teleimpressores Siemens T-1000 e Sagem.

No final da década de 80, início da década de 90 do século XX, foram instaladas nas maioria das UEO do Exército, as primeiras centrais de comutação de voz digitais, do fabricante português EID, cuja marca



ainda hoje é reconhecida como TÁGIDE, sendo então possível a sua integração com os novos rádios digitais, através de junções E&M ou através de acessos primários de 30 canais.

Estas centrais de comutação foram usadas na década de 90 em missões em que o Exército esteve presente, tais como na Bósnia, Kosovo e Timor, com grande sucesso, permitindo aos militares manterem o contacto com os seus familiares e amigos através da integração das cabines telefónicas do antigo operador Maxitel, utilizando para isso cartões pré-pagos.

Nestas missões, foram usados vários terminais satélite portáteis para garantir a ligação *Rear-Link* ao território nacional, e assim garantir a capacidade de Comando e Controlo em qualquer lugar e em qualquer altura, visto que a maioria destes terminais usavam ligações de órbita baixa aos satélites geoestacionários.

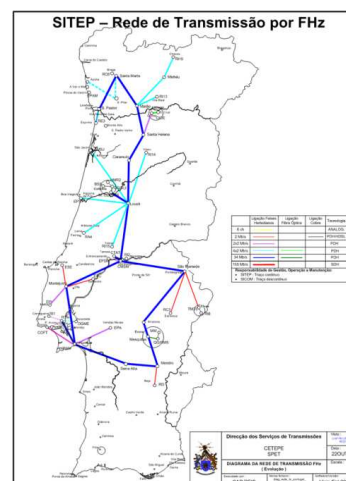
Com estes terminais era possível transmitir voz, dados e telefax, bastando no caso das comunicações de dados uma simples ligação a um computador pessoal, podendo a velocidade atingir os 9.6 kbps.

Posteriormente, em meados da década de 90, foram adquiridas ao fabricante canadiano MITEL, centrais de comutação de voz digitais, mais evoluídas tecnologicamente, e com dimensões mais reduzidas, permitindo uma otimização dos espaços disponíveis e dos consumos energéticos. A sua integração com a rede de voz do Exército era efetuada através de troncas digitais RDIS, de 15 ou 30 canais, conforme a largura de banda disponível.

Entre 1991 e 1997, foi implementada a primeira Rede de Transmissão digital por Feixes Hertzianos (FHZ), com tecnologia de multiplexagem PDH.

Em 1998 os teleimpressores foram substituídos por computadores pessoais, após o desenvolvimento de uma aplicação informática pelos militares da Unidade, para compatibilizar a central BEELINE com os computadores. Em 2003 devido à descontinuidade da BEELINE, foi também desenvolvido, por uma

equipa de militares da Unidade, um sistema de comutação automática de mensagens militares (SCAMM), suportado pela Rede de Dados do Exército (RDE).



Rede de Transmissão por FHZ

A RTE (Rede de Transmissão do Exército) foi implementada de forma a refletir a vocação de ocupação territorial conferida ao Exército e assim permitir a integração no SITEP de todas as U/E/O e também as Comunicações Táticas.

Em 2002, com o crescimento da RDE e a disponibilização de um maior número de serviços na área dos Sistemas de Informação surgiu a necessidade de efetuar o aumento da Largura de Banda no *backbone* da RTE por FHZ e de substituir os equipamentos de multiplexagem PDH por equipamentos SDH.

A primeira rede de Transmissão digital do Exército tinha a capacidade de *backbone* de 34 Mbps, e os *links* de FHZ para as U/E/O uma capacidade de 2 ou 4 Mbps (30 ou 60 canais) conforme o modelo do rádio. Os rádios utilizados nessa rede de transmissão eram do fabricante NERA, podendo em alguns casos, nas ligações terminais às UEO, ser do fabricante NOKIA.



Tecnologia

Sistemas Integrados de Serviços Digitais



Paulo Branco

Maj Tm (Eng)

“A sociedade de informação, presente na vida de qualquer cidadão, obriga a uma necessidade premente de aprendizagem dos novos conceitos e tecnologias nas áreas de comunicações e sistemas de informação...”

A informação sempre foi um veículo privilegiado de conhecimento e de poder político, económico e militar, desde os primórdios das civilizações. Com o desenvolvimento das tecnologias da informação e comunicação e o uso generalizado da Internet, os fluxos crescentes de informação mudaram a forma como funciona a economia (1), a governação, o comando e controlo, e as relações sociais, criando novos estilos de vida e de trabalho.

A implementação de qualquer sistema de informação deve obedecer, de forma resumida, aos seguintes objetivos estratégicos:

- **COMUNICAÇÃO** - Aumentar a capacidade de interação entre todos os intervenientes no processo;
- **COLABORAÇÃO** - Aumentar a capacidade de tratar e utilizar a informação;
- **EFICIÊNCIA** - Aumentar a produtividade através da automatização de processos e da redução ou eliminação da dependência do papel, contribuindo constantemente para uma eficaz desmaterialização;
- **TRANSPARÊNCIA** - Aumentar a capacidade de resposta através da ligação automática entre documentos e processos, e através da rapidez de acesso e consulta dos mesmos;
- **GESTÃO DO CONHECIMENTO** - Permitir uma maior capacidade de decisão, apoiada pelo sistema de informação e por todos os seus dados;
- **INOVAÇÃO** - Garantir a evolução das soluções, através da preparação da organização, e dos próprios sistemas, para evoluções futuras;
- **SEGURANÇA** - Garantir informação mais segura, por intermédio dos dispositivos de segurança disponibilizados pelos sistemas, e pelos mecanismos de comunicação;
- **INTEGRAÇÃO** - Garantir a integração com os sistemas e redes de comunicações existente.



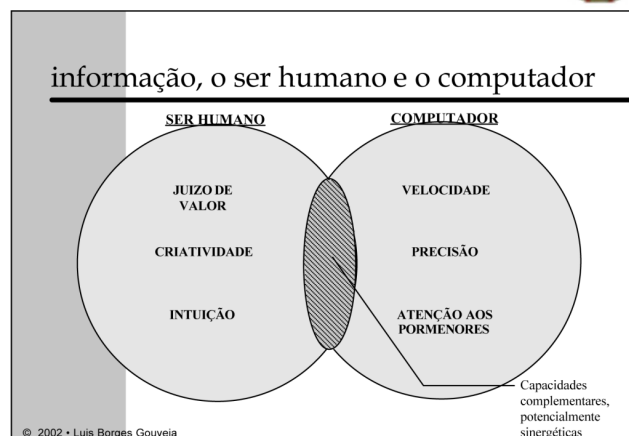


Com este modelo de serviços integrados torna-se possível apoiar e dinamizar o desenvolvimento de soluções tecnológicas avançadas a disponibilizar ao utilizador final. Para a implementação com sucesso de qualquer sistema de serviços digitais, desde o mais simples, como por exemplo, um portal colaborativo, ou mais complexo, tal como um sistema de armazenamento e salvaguarda de *Big Data*¹, devemos ter em atenção os seguintes critérios como pré-requisitos fundamentais:

- Instalação e gestão das infraestruturas de sistemas de comunicações e redes - atividade chave transversal de implementação de qualquer projeto de sistemas integrados;
- Possibilidade de existir um ponto de acesso generalizado ao sistema, pela Internet - atividade chave transversal que visa, tirar partido da disseminação da banda larga atualmente disponibilizada por qualquer ISP, e viabilizar a generalização do acesso e da utilização dos sistemas interligados com a rede pública, tais como o correio eletrónico e portais colaborativos com tecnologia WEB 2.02;
- Domínios aplicacionais verticais - atividade chave dirigida a áreas aplicacionais verticais recorrendo à utilização inovadora de tecnologias de informação avançadas.

As soluções, produtos e metodologias criadas deverão, em última análise, ser transmitidas e absorvidas pelos membros responsáveis pela área de administração em tecnologias de informação e respetivas delegações técnicas.

A relação entre o ser humano e as novas tecnologias pode ser representada pelo diagrama seguinte:



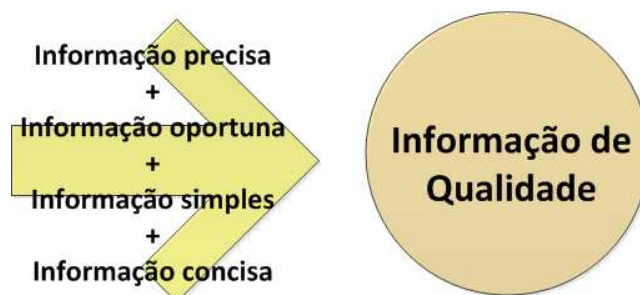
Um dos valores introduzidos neste conceito é a chamada “visão interna”, que procura durante o próprio desenvolvimento e implementação das soluções uma adaptabilidade ao objetivo em causa.

Uma das características principais das tecnologias de informação, é a utilização das ferramentas colocadas ao seu dispor de forma adequada para minimizar o esforço humano, simplificar os processos, diminuir as dificuldades de manipulação, e capacidade de lidar com excesso de informação.

As TI's podem ser decompostas em três componentes:

- Tratamento de informação
- Computadores
- Comunicações

Se o tratamento da informação for efetuado de forma eficaz, o resultado pode ser resumido da seguinte forma:



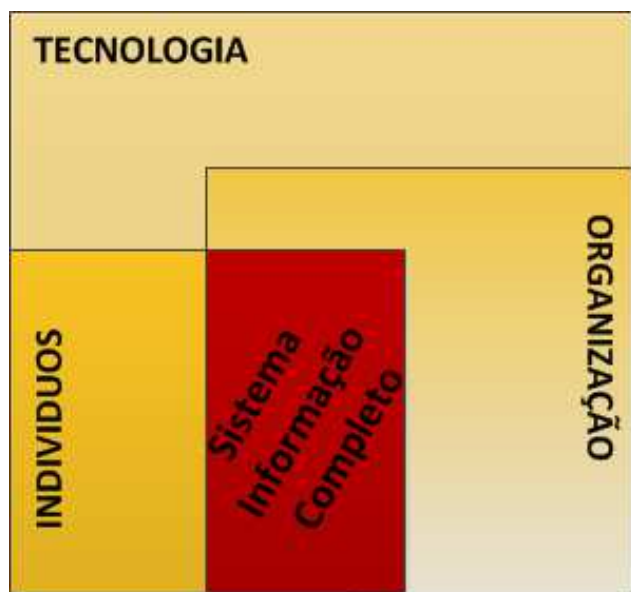
Esta informação é cada vez mais um trunfo no sucesso de qualquer organização, contudo essa

¹ Conceito, no qual o foco é o grande armazenamento de dados e maior velocidade. Podemos dizer que o *big data* se baseia em 5V's: Velocidade, Volume, Variedade, Veracidade e Valor.

² Termo criado em 2004 pela empresa americana O'Reilly Media para designar uma segunda geração de comunidades e serviços, tendo como conceito a "Web como plataforma", envolvendo *wikis*, aplicativos baseados em *folksonomia* (forma de indexação), redes sociais e Tecnologia da Informação.



capacidade de obter informação de qualidade, e que se traduz em clara superioridade no desenvolvimento do seu negócio, seja ele qual for, mesmo que militar, só é possível devido à existência de indivíduos que se traduzem em meios para atingir essas mesmas organizações, o que do ponto de vista das tecnologias de informação pode resultar num sistema de valor completo:



Desta forma, os Sistemas de Informação devem ser analisados e/ou desenvolvidos dentro da perspectiva sociotécnica, em que tecnologia e organização devem ser ajustadas entre si até que se obtenha uma harmonização perfeita entre os dois domínios, gerando um terceiro estado organizacional conjunto. (3)

Com base neste princípio essencial, qualquer sistema projetado segundo estas referências baseia-se numa solução *e-government* para unificação e integração.

Segundo o autor inglês Douglas Holmes, o *e-government* é mais do que tecnologia, mais do que *Internet* ou *contact-centers*, mais do que entrega de serviços.

É a capacidade de colocar os cidadãos e utilizadores no centro.

É, no fundo, um complexo mas extraordinário processo de CRM³ (*Customer Relationship Management*).

O "EGov" estabelece estratégias de *e-business* e as melhores práticas que podem ser replicadas em todo o sector público - governo central, governo local, educação, segurança pública, saúde, justiça, forças armadas e organismos supranacionais e intergovernamentais. Em cada estudo de caso, as organizações pretendem colocar os serviços e informações *online*, e assegurar o acesso fácil e universal a esses serviços e informações. Para tal, as organizações devem habilitar os seus funcionários a serem possuidores do conhecimento necessário, e trabalhar em parceria com outras organizações. Acima de tudo, o estado remove as barreiras para a sociedade da informação e lidera pelo exemplo. (4)

SERVIÇOS DIGITAIS – TIPIIFICAÇÃO APLICADA AO EXÉRCITO

VoIP

A tecnologia VoIP (*Voice over IP*) permite a realização de conversações telefónicas através de redes baseadas no protocolo IP, como por exemplo as redes estruturadas convergentes e a Internet.

Longe vão os tempos em que as infraestruturas de comunicação de voz e as de comunicação de dados eram consideradas dois mundos opostos. Com a evolução das tecnologias de comunicação e dos protocolos de suporte das grandes redes incluindo a Internet, é hoje possível o que há uma década atrás não passava de uma miragem: transportar voz em tempo real através das infraestruturas que suportam essas redes. (5)

Sendo potencialmente os mais afetados por este movimento de convergência, os fabricantes tradicionais de equipamentos para redes de voz têm

³ Processo criado para definir toda uma classe de ferramentas que automatizam as funções de contacto com o cliente (utilizador final), essas ferramentas compreendem sistemas informatizados e fundamentalmente uma mudança de atitude corporativa, permite ajudar as empresas e organizações a criar e manter um bom relacionamento com seus clientes.



procurado acompanhar a tendência, incluindo, no seu portfólio atual, ofertas completas de soluções de voz baseadas em protocolos da família TCP/IP⁴ (*Transmission Control Protocol/Internet Protocol*).

Aproveitando as potencialidades das tecnologias atuais de suporte às redes TCP/IP, têm surgido ultimamente um número significativo de ofertas de serviços VoIP para utilizadores finais. Estes tipicamente permitem, quer a realização de comunicações de voz entre utilizadores ligados a esta rede, através do mesmo operador VoIP, quer a comunicação com a rede telefónica tradicional – PABX⁵ (*Private Automatic Branch Exchange*), e também com as operadoras públicas, tanto ao nível da rede fixa, como móvel através de GSM (*Global System for Mobile Communications*), permitindo uma integração perfeita entre o mundo tradicional das comunicações de voz e os novos sistemas de telefonia IP.

A rede de comunicações de dados das forças armadas portuguesas é tecnologicamente avançada e com características que potenciam o desenvolvimento de novos serviços.

O projeto de comunicações IP surgiu com base neste enquadramento anterior, tendo como um dos grandes objetivos a implementação de tecnologias de VoIP ao nível da Rede de Dados das Forças Armadas, e a interligação com a rede telefónica *legacy* interna e qualquer rede telefónica externa (pública). (6)

Entre as principais vantagens identificadas para esta tecnologia, destacam-se:

- Custos mais baixos de comunicações;

- Possibilidade de integração da infraestrutura de rede, com a sua partilha, para os serviços de voz e de dados;

- Possibilidade de desenvolvimento de serviços avançados e sua integração com serviços existentes;

- Aumento da mobilidade dos utilizadores;

- Gateways de voz com qualquer operador da rede pública, fixa e/ou móvel;

- Alta disponibilidade;

- Qualidade de Serviço com priorização do tráfego de voz.



CORREIO ELECTRÓNICO

O serviço de correio eletrónico disponibiliza várias evoluções funcionais, nomeadamente em matéria de mobilidade. O acesso Web retoma a interface rica do cliente pesado e a gestão de terminais de tipo *pocket PC* ou *SmartPhone* permitindo uma integração de forma *standard*, por exemplo, conectar-se sem passar por uma VPN (*Virtual Private Network*) através de uma conexão segura HTTPS (*HyperText Transfer Protocol Secure*), com nível de encriptação RSA⁶ 2048 bits. O sistema atualmente em produção baseia-se no produto *Microsoft Exchange 2007*, podendo disponibilizar o *push* dinâmico, que permite uma sincronização ativa

⁴ Protocolo de Controlo de Transmissão/Protocolo Internet, é um conjunto de protocolos padrão para ligar computadores em redes.

⁵ Termo cuja tradução seria *Troca Automática de Ramais Privados*, é um centro de distribuição telefónica pertencente a uma organização/empresa que não inclua como sua atividade o fornecimento de serviços telefónicos ao público em geral.

⁶ É um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT, *Ronald Rivest*, *Adi Shamir* e *Leonard Adleman*, que inventaram este algoritmo com base num sistema de chaves assimétricas.



quando chegam novas mensagens. A isto acrescentam-se melhorias ao nível da administração, que passam a beneficiar da centralização da gestão, do arquivamento “a quente”, ou seja, sem ser necessário parar serviços, ou ainda de ferramentas que possibilitam verificar se todos os serviços necessários foram bem inicializados, se as correções de *software* estão atualizadas, se os serviços de rede funcionam bem, entre outros aspetos.

Um outro grande argumento da plataforma situa-se ao nível do seu forte potencial de consolidação. Deixou de haver um verdadeiro limite para o número de utilizadores e para o tamanho, tido como conveniente, das suas caixas de correio, sendo possível contudo uma restrição destes valores com base em políticas bem definidas por utilizador, ou grupo de utilizadores. A escalabilidade do sistema é uma garantia.



Os serviços de correio eletrónico possibilitam várias opções, para poder cobrir as necessidades reais que as organizações demandam: mais segurança e privacidade, opções de colaboração, gestão de contactos, acesso a agendas, gestão de tarefas, reuniões, etc. Assim como para responder às necessidades de mobilidade e acesso a estes serviços corporativos a partir de dispositivos fixos e móveis.

Com a plataforma de mensagens eletrónicas, obtemos uma solução profissional avançada para melhorar os serviços a disponibilizar:

- Comunicação mais eficaz na organização;
- Aumento da produtividade;
- Economia de custos;
- Maior segurança e privacidade no correio;

- Fiabilidade, segurança, tranquilidade;

- Acesso à plataforma desde dispositivos móveis e fixos em redes externas.

O sistema de correio eletrónico ajuda a organização a cumprir os requisitos regulamentares relacionados com a retenção de dados, incluindo requisitos de arquivo e de conformidade. Desta forma, ajuda a assegurar que as comunicações de correio eletrónico são corretamente controladas, arquivadas e identificadas.

Utilizar o Correio Eletrónico de forma profissional

Por vezes, os pormenores podem influenciar significativamente a forma como a organização encara os sistemas de informação:

- Assinaturas de correio eletrónico. Corresponde ao texto ou gráfico que pode ser colocado por baixo do nome numa mensagem de correio eletrónico. A criatividade é o limite;

- Anexar um vCard. Esta constitui uma outra forma de transmitir informações sobre a sua organização. Os vCard são o padrão da *Internet* para criar e partilhar cartões-de-visita virtuais. Pode criar facilmente um vCard no cliente de correio eletrónico e anexá-lo às mensagens enviadas;

- Assinatura Digital. Utilização de assinaturas digitais nos *emails* enviados, permitindo assim confirmar de forma inequívoca a sua identidade perante o sistema e garantir simultaneamente a integridade da informação enviada e recebida. Atualmente é possível usar qualquer certificado digital desde que aprovado e certificado pela entidade competente, tal como o certificado associado ao Cartão do Cidadão e também certificados gerados pela entidade certificadora do Exército ou do MDN;





- Agendar reuniões e sessões de videoconferência em tempo-real, permitindo o controlo das disponibilidades e dos intervenientes via mensagens de correio eletrónico.

Independentemente da maneira como é utilizado o correio eletrónico no sentido de favorecer os objetivos da organização, existem duas vantagens que gozam da estima de qualquer utilizador do sistema: o correio eletrónico é rápido e económico.

Políticas de correio eletrónico corretas e proteção por meio de Software

A implementação de políticas de correio eletrónico corretas para os utilizadores e a utilização de *software* adequado é necessário de forma a evitar embaraços, furtos, perda de informação – já para não falar da perda de produtividade individual e, no pior dos cenários, da própria organização.

Foram vários já os peritos em segurança informática que afirmaram que um computador seguro é aquele que permanece desligado. Todavia, esta alternativa é tão viável para as organizações como um hipotético regresso ao antigo sistema manuscrito, baseado em papel e em formas de correio mais demoradas.

As práticas e políticas sensatas de gestão de correio eletrónico ajudarão a organização a evoluir positivamente. Por exemplo, uma boa prática é utilizar uma política que especifica as mensagens de correio eletrónico que devem ser guardadas e/ou transmitidas e as que devem ser eliminadas, incluindo todas as mensagens consideradas SPAM (*Sending and Posting Advertisement in Mass*), ou seja, mensagens eletrónicas não solicitadas.

A primeira questão consiste em determinar a forma como serão guardadas as mensagens de correio eletrónico que são consideradas registos organizacionais importantes. Trata-se de um ponto fundamental no caso do correio eletrónico ser utilizado para transmitir informações de teor oficial ou tendo por base outra aplicação institucional que careça deste mecanismo de transporte para poder

ser usada, tal como a aplicação GESDOC atualmente em produção, fazendo parte dos SI do Exército.

PASTAS PARTILHADAS DE ACESSO RESTRITO e WEB SERVICES

O porquê de centralizar a informação

Para a maioria das organizações, a vantagem resulta da criação de um local central para alojar os dados críticos da organização. A consolidação dos seus dados críticos num só local assegura que os funcionários sabem onde encontrar e aceder às informações de que necessitam para se manterem produtivos. Significa igualmente que os seus dados são mais fáceis de proteger e copiar do que quando estão espalhados por uma série de computadores individuais. Esta funcionalidade está disponível nativamente com os sistemas operativos *Microsoft Server*, sendo apenas necessário efetuar as corretas configurações do sistema. Todas as UEOs do Exército dispõem desta possibilidade e na sua maioria são utilizadoras assíduas deste serviço, através dos serviços disponibilizados no seu servidor local, cuja responsabilidade de manutenção e salvaguarda da informação é inteiramente do Centro de Gestão de Sistemas do Regimento de Transmissões.



Uma *intranet* consiste num *Web site* interno da organização, no qual se pode publicar informações às quais apenas alguns utilizadores podem aceder, conforme permissões devidamente atribuídas. O sistema em produção no Exército tem por base o *Windows SharePoint Services* e o *SharePoint Foundation 2010*, da Microsoft, um programa que permite a um servidor alojar um *Web site* interno pré-configurado. Os utilizadores podem aceder ao *site* para publicar documentos e colaborar. Também pode utilizar o *site* para publicar comunicações, eventos, calendários e ligações para recursos importantes da organização. (7)



Colaboração de forma fácil e sem obstáculos

O *SharePoint Services* pode ajudar os utilizadores a colaborarem facilmente em projetos, mesmo que estejam em diferentes locais.

Imediatamente depois de criar uma conta, o *Web site* está pronto a ser utilizado, completo com uma página de informação, listas de debate *online*, notícias e bibliotecas de documentos.

Com um *Web site SharePoint* em funcionamento, todas as pessoas na organização podem:

- Partilhar informação de forma segura e trabalharem em conjunto;
- Enviar automaticamente mensagens de alerta aos elementos da equipa sempre que conteúdos forem alterados;
- Realizar debates *online* para uma colaboração mais fácil e revisão de documentos;
- Atribuir diferentes níveis de acesso aos utilizadores;
- Obter opiniões dos elementos da equipa através de consultas *online*;
- Gerir calendários de grupo, listas de contactos e informação;
- Partilhar imagens utilizando uma biblioteca de imagens.

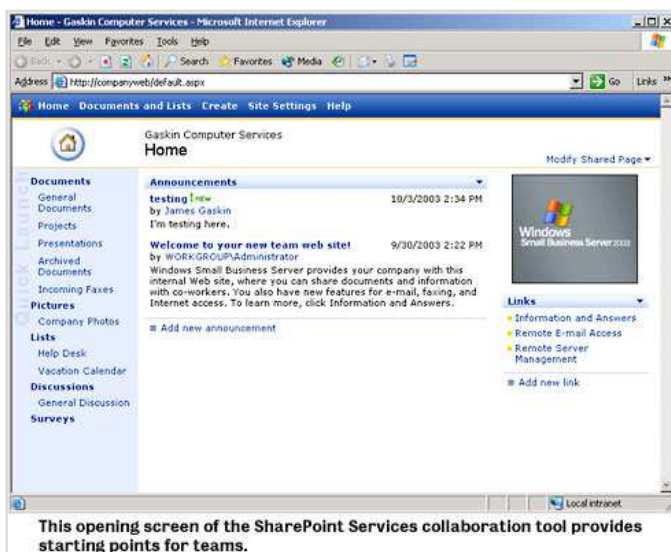
Facilitar a Partilha e Revisão de documentos

O acesso fácil a documentos importantes é sempre assegurado. A biblioteca de documentos permite o acesso a ficheiros em qualquer computador com uma ligação à RDE (Rede Dados do Exército) e um *browser* compatível. Adicionalmente, os elementos da equipa podem rever documentos e projetos através do *site*.

- Transferir documentos de qualquer computador para uma biblioteca de documentos *online*;
- Capturar, partilhar e desenvolver ideias, informações, comunicações, documentos, planos de negócio, fotografias, desenhos e muito mais;
- Debates *online* acerca de documentos sem os rever;
- Tirar partido de excecionais funcionalidades de suporte tais como subpastas, versões de ficheiros e controlo de entrada/saída (para que as alterações efetuadas por uma pessoa a um documento não anule as de outra);
- Adicionar eventos e informação para a sua organização ou equipa;
- Controlar tarefas e tópicos com listas personalizadas.

Sistemas de Calendários Partilhados

Algumas equipas tendem a subestimar a utilidade do sistema de calendários partilhados do sistema quando se trata de trabalhar à distância. O facto de as agendas se encontrarem disponíveis *online* permite aos utilizadores marcar as reuniões mediante o acesso às salas de reuniões virtuais e a consulta da disponibilidade dos participantes. Sem esta funcionalidade, teriam de contactar individual e diretamente todas as partes interessadas da reunião e, em seguida, comparar as agendas até encontrarem um horário comum disponível. Este processo não só contribui para o desperdício de





tempo útil como para o aumento de tempo em utilização da rede telefónica.

Áreas de Anúncios/Novidades

É possível automatizar o processo que permite informar os utilizadores das novidades por intermédio da publicação de anúncios diretamente em áreas de trabalho virtuais partilhadas. Este procedimento ajuda a diminuir a carga administrativa inerente à criação, encaminhamento e envio de anúncios impressos ou por correio eletrónico. Pode otimizar ainda mais este processo de comunicação mediante a criação de uma caixa de anúncios, de forma destacada, na parte superior do *Web site* colaborativo.

CONCLUSÕES

A sociedade de informação, que está permanentemente presente na vida de qualquer cidadão, quer de forma individual quer coletiva, obriga de forma direta e indiretamente a uma necessidade premente de conhecimento e aprendizagem dos novos conceitos e tecnologias emergentes nas áreas de comunicações e sistemas de informação.

Torna-se imperativo uma gestão eficiente da informação disponível, tal a sua vastidão. Calcula-se que, no início deste século, apenas cerca de 25% do total da informação arquivada no mundo estava sob forma digital e a restante preservada em papel, fotografia, filme e em outros meios. Atualmente, passado pouco mais do que uma década, essa percentagem aumentou para mais de 90%.

As redes de telecomunicações existentes hoje em dia facilitam a transferência desta informação de forma continuada e rápida. De acordo com a IBM, criam-se a cada dia no mundo aproximadamente 2,5 *exabytes* de informação, ou seja, $2,5 \times 10^{18}$ unidades de informação digital ou *bytes*.

É por isso de significado relevante o facto de qualquer organização procurar estar alerta às inovações e produzir constantemente atualizações

dos seus sistemas e processos para conseguir acompanhar a evolução normal das redes e sistemas de suporte ao seu *core business*.



Bibliografia

1. Santos, Filipe Duarte. <http://www.computerworld.com.pt/>. [Online] <http://www.computerworld.com.pt/2013/07/25/big-data-big-brother-e-snowden/>
2. Gouveia, Luis Borges. <http://www.ufp.pt>. [Online] <http://www.ufp.pt/~lmbq>
3. Rezende, Denis Alcides e Abreu, Aline França de. *Tecnologia da Informação aplicada a Sistemas de Informação Empresariais*. s.l. : Atlas, 2013
4. Holmes, Douglas. <http://www.dougholmes.com>. [Online] Nicholas Brealey Publishing, London, 2001. http://www.dougholmes.com/egov_ebusiness.html
5. Rodrigues, Nuno, Costa, Eduardo e Vale, Sérgio do. *VoIP@IPB – Piloto de Telefonía IP numa Instituição de Ensino Superior*. <https://bibliotecadigital.ipb.pt>. [Online] Instituto Politécnico de Bragança, Centro de Comunicações. https://bibliotecadigital.ipb.pt/bitstream/10198/611/1/voip_ipb.pdf
6. Branco, Maj Tm (Eng^o) Paulo. *A nova Rede de Transmissão do Exército*. Almenara. 2011
7. Microsoft. <http://office.microsoft.com>. [Online] <http://office.microsoft.com/pt-pt/sharepoint/>



Tecnologia

O SharePoint como uma plataforma de desenvolvimento para o Portal de Lições Aprendidas



Paulo Carvalho

Cap Tm (Eng)

“É o Portal das Lições Aprendidas, que depois de criado vem dar ao Exército a ferramenta necessária para operacionalizar todo este processo...”

... passa a conseguir direcionar todos os utilizadores envolvidos no processo de recolha e análise da informação e a maximizar o alcance e a rapidez da disseminação dos resultados...”

Existem uma série de tecnologias e ferramentas que quando combinadas tornam mais fácil do que nunca a criação de aplicações. Em geral, a *Microsoft* tem adotado uma estratégia unificadora canalizando o esforço principal do desenvolvimento de aplicações para a própria infraestrutura, tornando assim possível para quem pretende criar uma nova aplicação ser mais um *designer* e menos um programador, já que passou a ser simplesmente possível usar todos esses recursos no *SharePoint* de uma forma intuitiva e através da interface do utilizador.

Do lado das ferramentas, o *Office SharePoint Designer*, ou até o *Microsoft Visual Studio*, tornam possível estender as funcionalidades já existente num *site SharePoint* através da reutilização de blocos código (concebidos por outros) para fazer coisas que pela sua complexidade costumavam ser muito difíceis de realizar e por isso não estavam ao alcance de qualquer pessoa.

Do lado da tecnologia, o suporte de novos recursos como os fluxos de trabalho ou “*workflows*” significa que um *designer* não tem de escrever uma única linha de código para, por exemplo, conseguir criar um fluxo de aprovação numa aplicação.



Foram estas tecnologias e ferramentas que se uniram no processo de criação do Portal das Lições Aprendidas do Exército, começando por se desenhar o Portal recorrendo às funcionalidades e capacidades mais relevantes já existentes no *SharePoint* e que posteriormente foram estendidas:



Bibliotecas e Listas, que constituem um repositório para todos os dados no *SharePoint*, sejam eles ficheiros ou simplesmente dados estruturados. O *SharePoint* apresenta um conjunto de bibliotecas e certos tipos de lista, que podem ser usados como a base para as aplicações. Tipos de biblioteca que podem incluir algo tão original como uma biblioteca de slides, especialmente concebida para armazenar, gerir e apresentar de forma eficaz slides do *PowerPoint* da *Microsoft*, ou até uma biblioteca de ligação de dados utilizadas para interligar de modo fácil bases de dados de diferentes tecnologias e apresentar os seus dados completamente integrados.

Tipos de Dados ou **Content Types**, são um conceito central usado em todo o *SharePoint* e são projetados para ajudar os utilizadores a organizar o conteúdo dos seus sites de uma forma mais “inteligente”. Um tipo de conteúdo é uma coleção reutilizável de configurações que podem ser aplicadas a certas categorias de conteúdo. Os tipos de conteúdo permitem gerir centralmente e reutilizar os metadados e comportamentos de um documento ou as colunas de um item. Por exemplo, podemos associar desde logo os fluxos de trabalho e eventos a um tipo de conteúdo, ao invés de ter que adicionar posteriormente fluxos de trabalho e eventos em vários documentos ou bibliotecas.

Coluna de Site, que fornecem um modelo central, reutilizável para a definição de uma coluna. Quando é criada uma coluna de *site*, cada lista que usa essa coluna tem a mesma definição, e assim não é necessário ter que reproduzir a coluna em cada lista. As colunas de *site* permitem aos utilizadores finais escolher a partir de um conjunto pré-definido de colunas quais as que podem ser úteis nas suas listas. Assim, não só estas podem ser escolhidas para definir as colunas centrais de modelos de lista mais comuns, como também fornecer aos utilizadores um caminho para usar colunas especiais que podem ter significados personalizados.

Fluxos de trabalho, que permitem anexar um processo de negócio aos itens de uma lista ou biblioteca (forma natural de armazenar os dados no *SharePoint*). Este processo pode controlar quase qualquer aspeto de um

item, e incluir também o ciclo de vida desse item. Por exemplo, podemos criar um fluxo de trabalho simples, que encaminha um documento para uma série de utilizadores para aprovação. Normalmente, um *designer* do *site* vai necessitar de criar fluxos de trabalho específicos. Para tal o *designer* terá de usar o *Office SharePoint Designer* que irá oferecer um conjunto de fluxos mais completos, mas, ainda assim limitados. Contudo é possível ainda vestir a pele de um programador e usar o *Microsoft Visual Studio* para criar fluxos de trabalho realmente poderosos que, teoricamente, só estão limitados pela imaginação.

OFFICE SHAREPOINT DESIGNER: A PRINCIPAL FERRAMENTA PARA A CONSTRUÇÃO DA APLICAÇÃO

O *Office SharePoint Designer* é projetado especificamente para ajudar a criar e personalizar *sites* e fluxos de trabalho criados com produtos e tecnologias *SharePoint*. Ao utilizá-lo os *designers* e criadores de soluções que necessitam desenvolver as suas aplicações no *SharePoint*, tornam-se capazes de criar soluções que aumentam a agilidade organizacional e automação de processos de negócio. Usando o *Office SharePoint Designer*, não temos que usar linguagens de codificação processuais tradicionais ou técnicas para fazer o seguinte:

- Criar vistas e formulários de dados disponíveis numa variedade de fontes de dados - como ficheiros XML, bases de dados SQL, seja no *Microsoft SQL Server* ou não, ou simplesmente em *Web Services*;
- Criar sofisticados e dinâmicos fluxos de trabalho sem código;
- Desenhar *layouts* de páginas e aplicar folhas de estilo;
- Criar páginas mestras;
- Editar e aplicar folhas de estilo em cascata (CSS);
- Construir páginas de Peças Web e criar ligações entre Peças Web para criar aplicativos de negócios sofisticados.



O Desenvolvimento do Portal

Embora não tenha sido necessário ter um documento de especificações técnicas altamente detalhadas antes de construir a solução para o Portal das Lições Aprendidas com o *SharePoint*, foi fundamental ter uma boa ideia de como a aplicação iria funcionar. O ponto anterior pode parecer óbvio, mas muitos *designers* experimentaram a tormenta do desencontro entre as partes envolvidas, em que aquilo que os clientes querem na aplicação e o que eles realmente acreditam ser necessário para a aplicação ter sucesso está por vezes totalmente desfasado (e claro, os clientes geralmente só o percebem quando veem a aplicação quase acabada!).

Isto para dizer que partir do início significava reunir os requisitos funcionais e refletir sobre o que a aplicação precisava fazer. Neste caso queríamos identificar, no mínimo, o seguinte:

- Quais são os atores / funções no processo de criação das Lições Aprendidas? Neste caso, existem três atores diferentes. No topo, o proprietário do Portal que é a Repartição de Lições Aprendidas, representada pelos seus elementos. Num patamar intermédio os oficiais designados Oficiais de Lições Aprendidas – OfLA - de cada UEO do Exército. Por último, num patamar inferior, todos os colaboradores das Forças Armadas que tendo acesso às intranets dos Ramos se transformam em potenciais consumidores da informação disponibilizada.
- Quais são as necessidades de *User Interface* (UI) para os diferentes atores? Neste caso, o dono do Portal sobressai por necessitar de um controlo global sobre toda a informação contida na base de dados e ainda, por necessitar de uma ferramenta para gestão da lista de OfLA cuja correção e atualização são fundamentais para a atribuição de permissões corretas. Os OfLA por sua vez necessitam de filtros de informação baseados na origem dos dados para tratarem apenas os registos relacionados com a sua UEO. Aos restantes servirá a filtragem para

selecionar apenas os itens que não estando ainda aprovados sejam da sua autoria, ou que, estando já aprovados apareçam agrupados consoante o seu estado.

- Quais são as relações entre os dados? Neste caso, se olharmos para um item de projeto, observa-se que este nasce sempre na sua forma mais elementar com a inclusão de um conjunto de campos de dados considerados obrigatórios e que a este se atribui a designação de Observação. Depois, a esse item, que pode ser criado por qualquer colaborador de uma UEO, será associado um *workflow* de aprovação com um mecanismo de alerta dirigido ao OfLA dessa UEO. Depois de aprovado o item ficará em processamento e será sempre estudado de forma integrada pela Repartição de Lições Aprendidas e pelas partes julgadas interessadas até que o processo culmine na disponibilização a todos do documento formal contendo toda a informação relacionada com o processo de aprendizagem associado a essa situação ou matéria.
- Quais os mecanismos de alerta necessários? Para dispensar a consulta sistemática ao Portal por parte dos utilizadores, que vão interagindo no processo da transformação dos itens desde a sua forma mais incompleta, a de Observação, até à sua forma mais completa, a de Lição Aprendida, foram criados alertas. Estes alertas notificam, de forma seletiva, todos os interessados num determinado assunto de que um novo item foi criado, de que um item foi modificado ou que simplesmente foram criados comentários extra pelos visitantes do Portal.

Validar o modelo de dados

No caso presente, o modelo de dados implementado não requereu uma análise muito profunda já que se baseia inteiramente no modelo já utilizado na base de dados de Lições Aprendidas do *Joint Analysis Lessons Learnt Center* – JALLC – da OTAN situado em Monsanto. Considerou-se que uma das características desejáveis seria a interoperabilidade entre os dois sistemas garantindo-se espaço para futura partilha de informação.



DETERMINAR OS COMPONENTES E SUAS RELAÇÕES

Por último, apresenta-se de forma sucinta, a descrição do processo de Lições Aprendidas baseada na doutrina de referência adotada pela Repartição de Lições Aprendidas. Conhecendo o processo e conhecendo a terminologia envolvida no mesmo, fica-se com uma boa ideia da descrição funcional da aplicação.

Terminologia das Lições Aprendidas

Observação - É um comentário baseado em algo que alguém ouviu, viu ou leu, que foi identificado e registado como um assunto para melhoria ou uma potencial boa prática.

Boa Prática (BP) - é uma técnica, processo ou metodologia que contribui para a melhoria do desempenho de uma organização tendo sido identificada como o "melhor modo de operar" numa determinada área. Idealmente, uma Boa Prática deve ser adaptável, reproduzível e de utilização imediata.

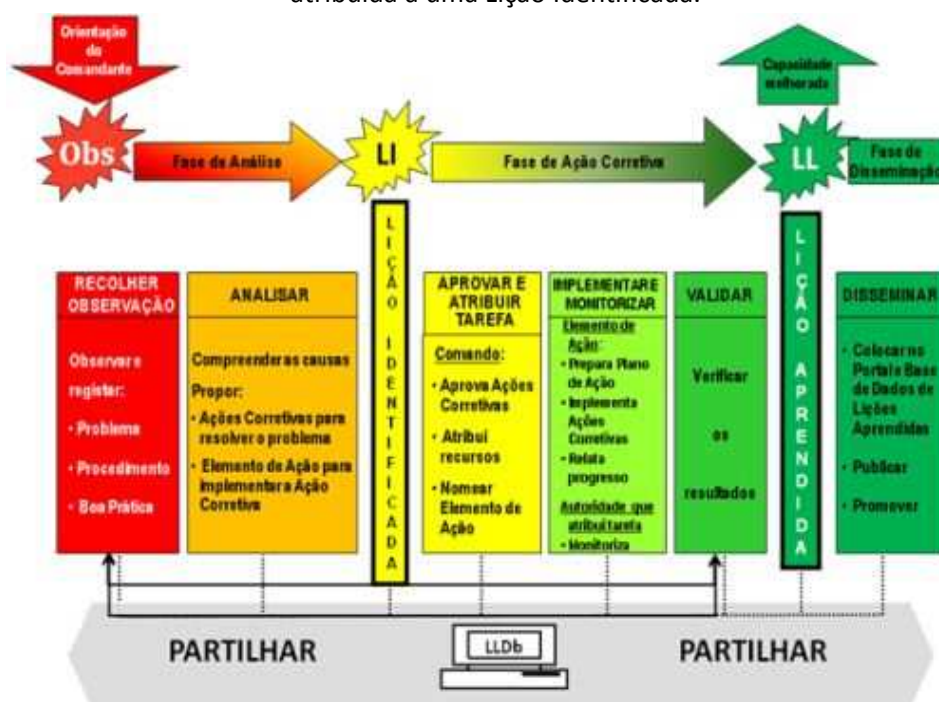
Lição Identificada (LI) - É uma observação com uma causa raiz determinada para o assunto observado, uma ação corretiva e uma entidade de ação recomendados, que foram desenvolvidos e propostos à autoridade apropriada.

Ação Corretiva (AC) - É uma atividade ou conjunto de atividades que corrige um assunto identificado para melhoria ou facilita a implementação de uma boa prática.

Entidade de Ação (EA) - É a organização ou pessoa nomeada para implementar a Ação Corretiva atribuída em associação com a Lição Identificada. O Elemento de Ação elabora um Plano de Ação para guiar as atividades inerentes à Ação Corretiva.

Lição Aprendida (LA) - É uma capacidade melhorada ou um melhor desempenho em qualquer um dos domínios do conhecimento militar (DOTMLPF-I⁷), confirmado(a) pela validação quando necessária, resultante da implementação de uma ou mais Ações Corretivas para uma Lição Identificada.

Plano de Ação (PA) - É o documento escrito com as atividades e etapas estabelecidas por um Elemento de Ação para implementar a Ação Corretiva atribuída a uma Lição Identificada.



O PROCESSO DE LIÇÕES APRENDIDAS NO EXÉRCITO PORTUGUÊS

O processo de criação de Lições Aprendidas no Exército segue três etapas genéricas da base de aprendizagem: a "**Identificação**" que ocorre durante a fase da análise do processo de transformação da Observação em Lição Identificada e a "**Ação**" e a "**Institucionalização**" que ocorrem durante a fase do processo que transforma a Lição Identificada em Lição Aprendida. No Exército, a "Institucionalização" é vista como parte integrante da ação necessária para alcançar uma Lição Aprendida. A informação

⁷ DOTMLPF-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Instalações e Interoperabilidade)



gerada durante o Processo de Lições Aprendidas pode e deve ser partilhada a qualquer momento, conforme os fluxos de trabalho pré-estabelecidos, e que determinam a forma como a capacidade de LA deve ser gerida nos diferentes patamares de responsabilidade.

A Fase de Análise é a primeira do Processo de Lições Aprendidas e tem como objetivo produzir uma Lição Identificada. Começa com a recolha de uma observação/boa prática e termina com a análise da mesma. A análise permite descobrir a(s) causa(s) do problema observado ou simplesmente o sucesso do mesmo. Após a compreensão da causa, pode ser identificada uma Ação Corretiva adequada para corrigir o problema ou manter o sucesso. A pessoa ou organização (denominada por Elemento de Ação - EA) que deverá executar a Ação Corretiva (AC) também será identificada durante a Análise.

Na Fase da Ação Corretiva, as LI desenvolvidas serão apresentadas à liderança da organização para que a mesma determine como prosseguir com a LI no Processo de Lições Aprendidas. Primeiro, a LI será aprovada e atribuída para ação posterior e a AC proposta é aceite ou modificada. De seguida será nomeado um EA para planear e implementar a AC e serão atribuídos os recursos necessários para a implementação. Durante este passo do Processo de Lições Aprendidas, o EA elabora um Plano de Ação para guiar as atividades decorrentes da implementação da AC. O Oficial de LA (OfLA) suporta a liderança monitorizando a implementação. Depois da AC ter sido implementada, realiza-se a validação, se necessário.

Com a Fase da Disseminação culmina o Processo de Lições Aprendidas. Após a validação da Lição Identificada para que esta se torne numa Lição Aprendida, inicia-se a Disseminação e publicação da informação obtida, para que os interessados tenham acesso à mesma. Embora a figura mostre a disseminação como sendo o passo final do processo, a partilha da informação proveniente do Processo de Lições Aprendidas deve ocorrer ao longo de todo o processo.

Métodos de Recolha de Observações

Uma observação é a base do processo de Lições Aprendidas. Uma das tarefas mais importantes dos OfLA é recolher observações da organização à medida que ocorrem, especialmente após atividades ou eventos planeados. Todo o pessoal, independentemente do posto ou categoria, deve entender que tem a responsabilidade de registar problemas, falhas e sucessos observados.

O Formato ODCR

Um dos métodos de recolha passa pela utilização do formato ODCR (Observação, Discussão, Conclusão e Recomendação). O uso deste modelo comum permite que a informação seja partilhada mais facilmente, nomeadamente por via da transferência automática de dados.

Relatórios Pós-Evento

Os relatórios elaborados após os eventos são um meio ideal para obter observações. A Diretiva dos Exercícios complementada por diretivas específicas e NEP dos comandos envolvidos dão orientações específicas sobre o formato e o cronograma para a produção de relatórios pós-evento, incluindo relatórios internos. Estes relatórios podem conter muita da informação necessária para registar observações.

Entrevistas Pós-Operação e Pós-Exercício

As entrevistas após operação ou exercício são uma maneira valiosa para obter observações, lições e boas práticas antes das tropas e dos principais líderes dispersarem e enquanto as memórias dos eventos permanecem claras. As entrevistas têm a vantagem adicional de permitir que o entrevistador se concentre em áreas de interesse que o entrevistado poderá considerar não importantes.

Métodos de Difusão

O valor do processo de Lições Aprendidas só é percebido quando a informação gerada pelo processo está disponível para quem e quando



necessita dela. A disseminação de LA e a partilha de informação gera conhecimento na organização e conduz a uma melhoria permanente do desempenho da mesma.

Perante a sua organização, o OfLA é responsável pela disseminação e partilha de informação proveniente do Processo de Lições Aprendidas.

Através da Comunidade de Interesse

As comunidades de interesse, comprometidas com uma aprendizagem social, são constituídas por pessoas com objetivos comuns que interagem umas com as outras. No âmbito militar, as oportunidades para interagir incluem conferências, reuniões de trabalho, grupos e trabalho e, naturalmente, a comunicação direta. Muitas comunidades de interesse são apoiadas pelos fóruns que lhes permitem partilhar as suas experiências. A participação em fóruns permite reforçar os contatos pessoais para encorajar a partilha da informação.

Serviços de Pedidos de Informação

Algumas organizações disponibilizam um serviço de pedidos de informação, onde quem necessita de informação sobre um determinado assunto pode fazer um pedido ao órgão de Lições Aprendidas (como por exemplo a RepLA) que procurará a informação disponível para responder ao pedido.

Treino

Os eventos de treino no início das rotações para um determinado teatro, no início dos exercícios, ou como parte da apresentação para um novo cargo são boas oportunidades para informar o pessoal sobre os benefícios, oportunidades e exigências de um processo de Lições Aprendidas, bem como para os informar sobre as últimas lições do terreno.

Publicações

Além dos relatórios de rotina (por exemplo, *After Action Review*, relatórios de missão periódicos,

relatórios de final de exercício, etc.), existem várias maneiras de garantir que a informação proveniente do processo de Lições Aprendidas chega ao pessoal da organização e exterior à organização. A informação pode ser compilada em:

- Publicações doutrinárias
- Relatórios
- Boletins informativos
- Brochuras/Folhetos/Cartazes/Placards informativos
- E-mails

Tecnologias da Informação

Existem várias ferramentas de tecnologias de informação que suportam a partilha de lições e informação, onde se incluem:

- Portais;
- Bases de dados, por exemplo a LLDb do Exército;
- Repositórios de conhecimento, como Wikis;

É o Portal das Lições Aprendidas, que depois de criado vem dar ao Exército a ferramenta necessária para operacionalizar todo este processo. A Repartição das Lições Aprendidas, assumindo a gestão desta ferramenta passa a conseguir direcionar todos os utilizadores envolvidos no processo de recolha e análise da informação e a maximizar o alcance e a rapidez da disseminação dos resultados obtidos através do estudo e sistematização dos problemas. Com o tempo, os resultados irão decerto aparecer, e o período de testes já levado a cabo deixa-nos muito otimistas.



Tecnologia

Sistema de Videoconferência do Exército



Lopes Silva

Cap Tm (Eng)

“A Videoconferência é uma tecnologia que permite o contacto visual e sonoro entre pessoas que estão em lugares diferentes, dando a sensação que os interlocutores se encontram no mesmo local...”

A Videoconferência é uma tecnologia que permite o contacto visual e sonoro entre pessoas que estão em lugares diferentes, dando a sensação de que os interlocutores se encontram no mesmo local. Permite não só a comunicação entre um grupo, mas também a comunicação pessoa-a-pessoa.

Desde sempre que o Exército se deparou com a necessidade de reuniões que incluem militares de Unidades de diferentes partes do país. O deslocamento destes militares para uma só unidade tem duas grandes desvantagens:

- Tempo gasto em viagens; tempo perdido pelos militares no deslocamento para um local específico;
- Gastos de recursos; viaturas, gásóleo, guias de marcha.



O primeiro Órgão Central de Administração e Direção (OCAD) a demonstrar necessidade de um sistema de videoconferência foi o Comando das Forças Terrestres (CFT), muito devido a ter sob o seu comando as Forças Nacionais Destacadas (FND), o Comando da Zona Militar dos Açores e o Comando da Zona Militar da Madeira. Com o enorme sucesso sentido no CFT, o Exército decidiu equipar toda a sua estrutura com este sistema.

O funcionamento de um sistema de videoconferência, do ponto de vista do utilizador, deve ser o mais convívil possível e deve implicar apenas um número limitado de operações, p. ex.: ligar e desligar câmaras e microfones, estabelecer a ligação via um menu de seleção, estabelecer a configuração através do menu de aplicação, terminar a ligação e iniciar/encerrar a sessão.

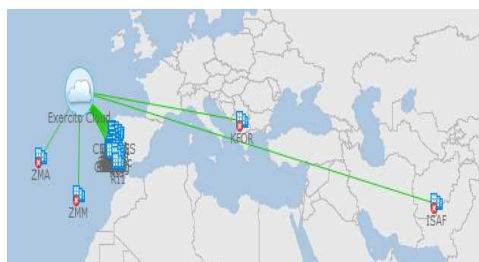
Com o rápido aumento do número de terminais e da exigência dos utilizadores, foi necessário encontrar uma solução que satisfizesse os utilizadores e permitisse ao mesmo tempo manter o controlo do sistema. Neste sentido, foi adquirida a aplicação *Converged Management Application* (CMA), que entre outras, tem as seguintes funções:

Monitorização de todos os dispositivos do sistema de videoconferência (Terminais e *Multipoint Control Unit* (MCU));

Contém ferramentas que permitem aos Administradores programarem e acompanharem as atualizações de *software* e *firmware* de centenas de terminais em simultâneo;

Os administradores podem elaborar relatórios e gráficos detalhados sobre todas as videoconferências realizadas;

Gestão da lista telefónica da rede de videoconferência.



-

- 

- 

-

A ALMENARA Nº 5 – 2013 | 29



Tecnologia

Protocolo de Autenticação na Web - OpenID



Machado Custodio

Maj Inf

Mestre Eng^a Informática

“O OpenID é uma tecnologia grátis e descentralizada de single sign-on, que simplifica a interação online do utilizador na web eliminando a necessidade deste possuir um nome de utilizador e palavra passe para cada sítio da internet.”

No âmbito da segurança da informação, o controlo de acessos é composto por processos de autenticação, autorização e auditoria, com vista a permitir ou negar o acesso de um sujeito a um determinado objeto ou recurso do sistema. A autenticação permite identificar quem acede ao sistema, a autorização determina o que o sujeito pode efetuar sobre determinado recurso, e a auditoria permite verificar os recursos que o sujeito acedeu ou tentou aceder.

A generalidade dos atuais sítios da *internet* permitem o acesso de utilizadores anónimos a um conjunto de funcionalidades que se assumem sem criticidade, sendo contudo barrado a outras funcionalidades ou recursos. Para acede-los é então necessário que o utilizador se identifique perante o sistema, que este o autentique e verifique se tem autorização para ver ou manipular o recurso pretendido. As aplicações informáticas necessitam assim de um eficaz controlo de acessos, de forma a impedir o seu acesso a utilizadores não autorizados ou a limitar utilizadores autorizados a alguns recursos protegidos. Na identificação o utilizador apresenta ao sistema a sua identidade, sendo esta verificada através de uma credencial durante a autenticação.

De acordo com Matt Bishop (Bishop, 2005) existem 4 categorias de credenciais de autenticação: de conhecimento, como uma senha; de posse, como um cartão de acesso; de localização, como por exemplo o acesso a partir de um determinado computador; e de biometria, como por exemplo a iris. Os sistemas computacionais utilizam uma ou mais destas categorias de credenciais.

Apesar dos progressos ao nível da identificação biométrica, na generalidade das aplicações *web* a autenticação é efetuada recorrendo normalmente à categoria de conhecimento, no qual é solicitado o nome de utilizador e palavra passe, permitindo despoletar o processo de controlo de acesso. O maior problema desta categoria reside no facto da possibilidade das credenciais ficarem comprometidas. Como os sistemas de autenticação necessitam de guardar a informação de autenticação para poderem efetuar a validação das identificações, é vital que estes guardem essa informação de forma segura.

O Problema

Com a generalização do uso da *internet* os utilizadores acedem a cada vez mais aplicações, necessitando de memorizar várias credenciais. Ao utilizar em vários sítios o mesmo nome de utilizador e palavra passe, o utilizador incorre num grave risco de segurança. Como tradicionalmente cada palavra passe é guardada centralmente, se ocorrer um comprometimento de segurança num dos sítios, os outros poderão ser facilmente afetados.



A dificuldade na gestão e memorização destes identificadores digitais levou ao aparecimento do *single sign-on*. Este foi definido por Jan Clercq como a possibilidade de um utilizador se autenticar uma única vez perante uma autoridade de autenticação e depois poder aceder a outros recursos protegidos sem necessidade de uma nova autenticação (Clercq, 2002).

O sistema de *single sign-on* tem apenas um conjunto de credenciais por utilizador, tornando a tarefa da gestão de senhas bastante mais simplificada. O custo de desenvolvimento de novas aplicações é desta forma mais reduzido pois não tem necessidade de ter os seus próprios mecanismos de autenticação.

Contudo, existem dois problemas nesta solução. O primeiro reside no facto de ao existir uma falha de segurança no sistema de *single sign-on*, esta compromete todas as aplicações que a utilizam. O segundo problema surge no nível de segurança garantido, pois as aplicações ao partilharem a mesma infraestrutura de autenticação partilham também o mesmo nível de segurança.

Tecnologia OpenId

O *OpenID* é uma tecnologia grátis e descentralizada de *single sign-on* para a *internet*, que simplifica a interação *online* do utilizador na *web* eliminando a necessidade deste possuir um nome de utilizador e palavra passe para cada sítio da *internet*. Desta forma, é possível apenas com uma única conta autenticar-se em variados sítios, possibilitando ainda a partilha de alguma informação pessoal entre estes aquando da autenticação. Em 2005, Brad Fitzpatrick, formulou um protocolo para permitir autenticação no *Livejournal.com*, referindo-o como Yadis “*Yet another distributed identity system*”, sendo que mais tarde foi renomeado de *OpenID* (Recordon, et al., 2006). Basicamente, em sítios que suportam o *OpenID*, é possível um utilizador efetuar a sua autenticação, sem a criação de novas palavras passe, utilizando apenas uma conta sua já existente noutro sítio provedor de identidade, como por exemplo no *Gmail*, o serviço de *webmail* do Google.

Em 2007 foi criada a *OpenID Foundation*, disponível em <http://www.openid.net/foundation/>, com vista a suportar e promover a aplicação desta tecnologia na *web*. A partir de Fevereiro de 2008, após grandes empresas tecnológicas como a Microsoft, IBM, Google, Yahoo e Verisign se terem tornado membros desta fundação, esta solução foi sendo massivamente adotada pelos sítios da *internet* e respetivos utilizadores.

Existem 2 entidades no protocolo, o Provedor de Identidade e a Entidade Confiante. A primeira é responsável pela autenticação dos utilizadores, confirmando a identidade do utilizador à Entidade Confiante. A segunda é um serviço existente nas aplicações *web* que utiliza o protocolo *OpenID* para comunicar com um Provedor. Esta separação permite aos utilizadores escolherem o Provedor que desejem para efetuarem a autenticação. Desta forma a palavra passe é apenas fornecida pelo utilizador ao Provedor. Para se utilizar este protocolo, o utilizador necessita previamente de criar uma conta num dos Provedores existentes, como por exemplo Google, Yahoo, Facebook, AOL, etc. Quando o utilizador acede a uma aplicação que necessita de autenticação, a Entidade Confiante pede-lhe o seu identificador. Este identificador deverá ser um URL, como por exemplo <http://openid.aol.com/USERNAME> ou <https://www.google.com/accounts/o8/id> para contas respetivamente no AOL ou no Google. Este identificador permite à Entidade Confiante descobrir o Provedor associado, e redirecionar o utilizador para este através de um pedido de autenticação em HTTP. O Provedor pode livremente escolher o método de autenticação, pois não é especificado pelo protocolo. Após a autenticação, o Provedor redireciona o utilizador de volta para a Entidade Confiante. O sucesso da autenticação é descrito nesta mensagem de resposta. Quando a Entidade Confiante recebe esta resposta necessita de verificar a sua assinatura. Para este efeito, pode utilizar uma chave previamente acordada com o Provedor ou então reenviar-lhe a resposta, esperando que este a verifique e desta forma autentique o utilizador.



Fases do Protocolo OpenId

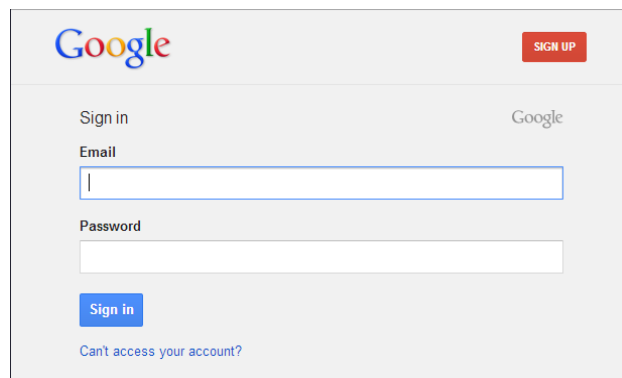
As figuras seguintes mostram exemplos de várias aplicações nas diversas fases do protocolo. A primeira figura é uma simples janela de login de uma aplicação que utiliza *OpenID*, na qual é pedido ao utilizador para escolher um Provedor de Identidade através do URL. Neste exemplo, o utilizador escolhe o URL <https://www.google.com/accounts/o8/id> que corresponde ao Google.



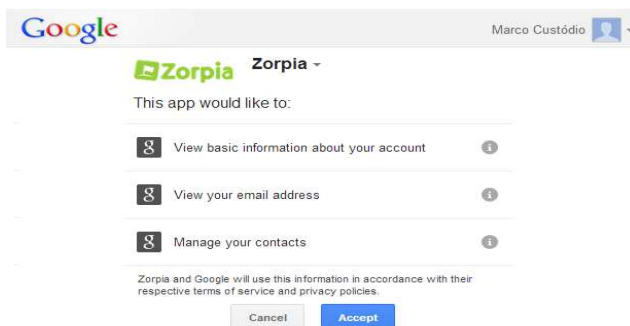
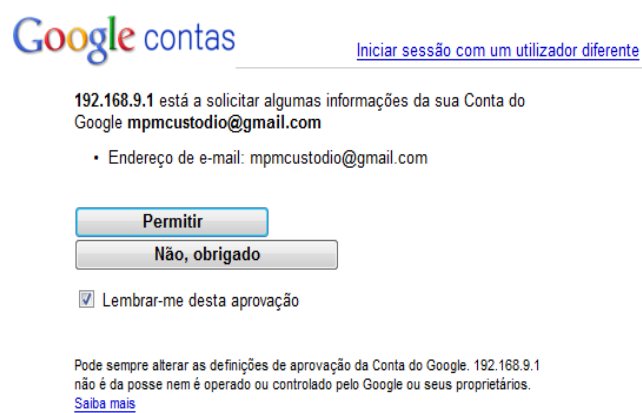
De referir que atualmente os utilizadores não necessitam de saber os URL dos seus provedores. A figura seguinte mostra um conjunto de Provedores de Identidade disponíveis ao utilizador necessitando apenas de clicar no respetivo ícone. Neste exemplo os seus URL's estão encapsulados na aplicação de modo que o utilizador não necessita de os memorizar.



Na figura abaixo podemos observar o ecrã que é apresentado ao utilizador pelo Provedor de Identidade Google, após o utilizador ter sido redirecionado para este. De notar que neste caso o utilizador ainda não estava autenticado no Google pelo que necessita de introduzir o seu *email* e palavra passe.



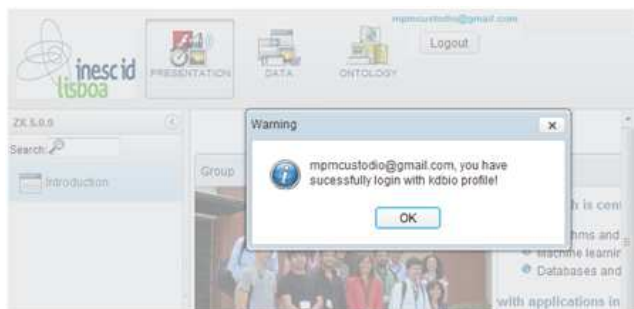
As figuras seguintes referem-se à situação em que o utilizador tenha previamente efetuado a sua autenticação no Gmail e a respetiva conta esteja ainda ativa, não necessitando de introduzir a sua palavra passe. Na primeira, o utilizador é inquirido sobre a permissão do Google fornecer o endereço de *email* à aplicação cujo IP é 192.168.9.1. Já no caso seguinte, a aplicação Zorpia pretende aceder ao endereço de email, à informação básica sobre a conta e ter a possibilidade de gerir os seus contactos.



A última figura demonstra a autenticação com sucesso, sendo o utilizador novamente



redirecionado para a aplicação original que solicitou a autenticação.



Conclusões

Do ponto de vista do utilizador, o uso do *OpenID* permite simplificar o processo de registo e autenticação nos vários sítios que visita, pois o Provedor de identidade para além de assegurar a identidade de utilizador pode também partilhar parte da sua informação genérica como nome, data de nascimento, morada, etc. A necessidade de atualização desta informação apenas carece de ser devidamente alterada num único local, no Provedor. Normalmente os Provedores estão alojados em arquiteturas computacionais sólidas de grandes empresas, na qual é dada primordial importância à questão da segurança informática, e assim, a proteção da identidade *online* dos seus utilizadores estará mais salvaguardada. Na eventualidade do comprometimento da palavra passe, como esta não é partilhada, apenas necessita de modificação no Provedor.

Bibliografia

Bishop, Matt. 2005. *Introduction to Computer Security*. s.l. : Addison-Wesley, 2005. ISBN: 0-321-24744-2.

Clercq, Jan De. 2002. *Single Sign-on Architectures*. s.l. : in *Infrastructure Security International*, 2002.

Recordon, David e Reed, Drummond. 2006. *OpenID 2.0: A Platform for User-Centric Identity Management*. Alexandria, Virginia, USA, : in *Conference on Computer and Communications Security Proceedings of the second ACM workshop on Digital identity management*, 2006.



Tecnologia

A Segurança de Informação e a Gestão de Eventos

De uma visão parcial para uma visão integrada



Rafael Aranha

Cap Tm (Eng)

“... em organizações com diversos tipos de sistemas ... é, fulcral ter-se um único ponto de recolha de informação ... onde se possa ter uma visão global e holística da Segurança dos SIC e da segurança da informação....”

Os atuais Sistemas de Informação e Comunicações (SIC), sejam estes materializados por serviços, aplicações e/ou equipamentos, produzem uma quantidade elevada de informação através dos denominados *logs*⁸. Estes *logs* informam o administrador ou o analista desses sistemas sobre os acontecimentos registados, doravante designados de eventos. Exemplos destes eventos podem ser o *login* de um utilizador, a criação de uma conta, a ativação de um serviço, tentativas de acesso não autorizadas, a deteção de vírus, a temperatura do equipamento, a ocupação do processador e memória, o ligar/desligar de uma porta num *switch*, a saturação de uma ligação num *router*, entre muitos outros.

O mundo dos Logs!

Por norma, uma organização tem diversas consolas de gestão e monitorização (G&M), dedicadas a cada um dos seus sistemas, onde recebem os *logs* e geram informação para que possa ser analisada por um analista – caixas azuis na figura seguinte. A quantidade de informação gerada pelos *logs* pode no entanto tornar-se avassaladora chegando facilmente a *GigaBytes* num mês. Desta forma, é humanamente incomportável a sua análise manual sendo necessário a utilização das referidas consolas⁹.

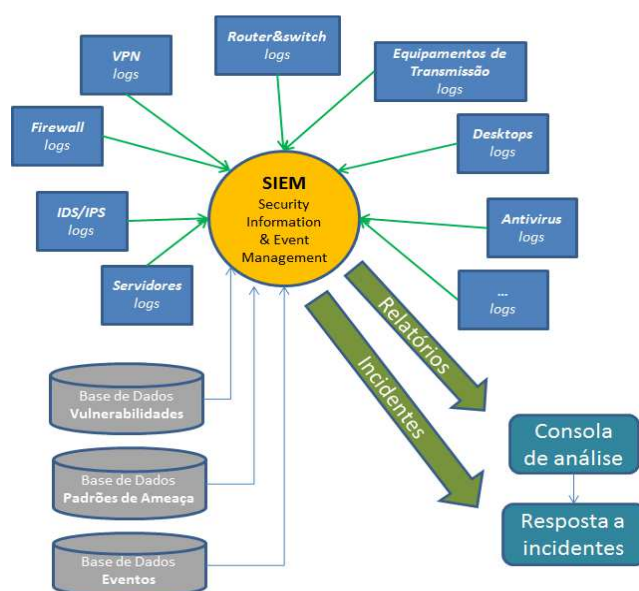


Diagrama lógico de alto nível dos componentes de um SIEM (Adaptado de Unisys)

⁸ O termo *log* advém de *logfile*. Estes são ficheiros onde são guardados os eventos registados por uma aplicação ou equipamento.

⁹ Em alguns casos é mesmo necessário a análise dos *logs* em formato *raw*. Exemplo disso é num contexto de análise forense.



Exemplos destes sistemas são as consolas de monitorização de uma solução de antivírus, consolas de G&M de equipamentos de rede (e.g. *routers*, *switch*, concentradores de VPN), consolas de G&M de equipamentos de segurança (e.g. *firewall*, IDS/IPS, *sniffers*) consolas de G&M de equipamentos de transmissão (e.g. equipamentos de Feixes Hertzianos, Fibra ótica, DSL, satélite, pontos de acesso de redes sem fios), consolas de gestão de serviços de diretório, nomes e servidores *web* (e.g. LDAP, AD, DNS, IIS, Apache), consolas de G&M de *Call Centers*, máquinas virtuais, etc.

No entanto, facilmente se depreende que, no respeitante à segurança da informação no contexto de uma organização, todos esses sistemas de G&M revelam uma visão parcial e localizada de um determinado evento. No entanto, a este evento, analisado de uma forma isolada, pode não ser dada a importância que, caso se tivesse uma visão integrada de todos os sistemas de G&M, ele mereceria.

Da necessidade de se ter uma visão integrada da segurança, conforme atrás apresentado, assim como da obrigatoriedade de muitas organizações

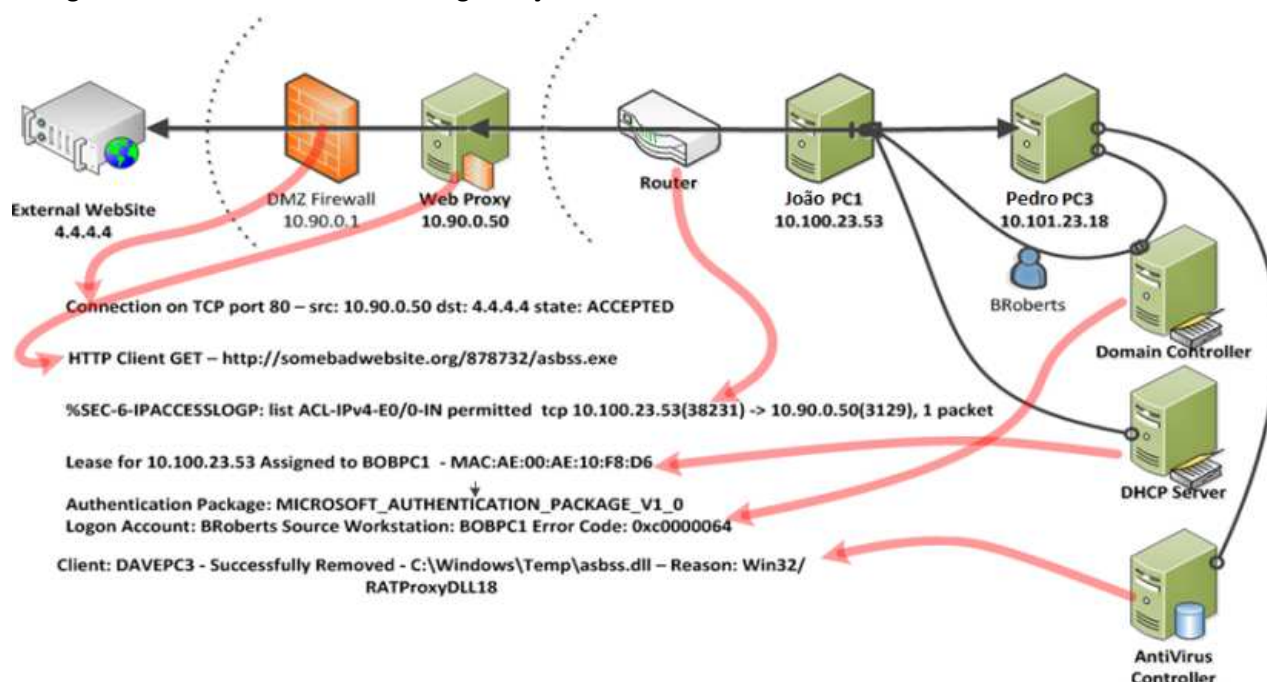
cumprirem normas de entidades reguladoras (e.g. ISO27001, PCI DSS¹⁰, Lei Sarbox, etc.), advêm os *Security Information and Event Management Systems* (SIEM). De uma forma simples, um SIEM recebe *logs* de praticamente todos os sistemas e equipamentos de uma organização, normaliza-os, correlaciona-os e gera alertas sobre ameaças aos SIC da organização. Desta forma, o SIEM é o único sistema capaz de ter uma visão integrada ao nível da segurança de informação de toda uma organização, conforme ilustrado na figura apresentada anteriormente.

O que parece nem sempre é!

De forma a ilustrar o anteriormente exposto apresenta-se o exemplo seguinte.

Os diversos serviços e equipamentos que compõem a rede ilustrada registaram nos seus *logs*, de forma diferente e em níveis distintos da camada OSI, um determinado evento. Este evento poderá ter sido apresentado nas diversas consolas de cada serviço ou equipamento, a um analista.

No entanto, salienta-se que algumas destas entradas são normais se analisadas fora de um determinado



Análise de logs gerados por diversos sistemas e equipamentos de uma organização (Fonte: OSSIM)

¹⁰ Payment Card Industry Data Security Standard.



contexto (e.g. as entradas registadas pela *firewall*, *router*, servidor DHCP).

Desta forma, numa organização onde todos os *logs* gerados são recolhidos, normalizados e correlacionados por um SIEM, o seguinte alarme seria gerado:

O PC1 onde o João está ligado foi infetado pelo ficheiro asbss.exe que teve origem num site que continha malware. Este malware utilizou as permissões do João para infetar o PC3 do Pedro. O antivírus detetou essa infeção. No entanto o PC1 está ainda infetado.

Desta forma, as conclusões que se retiram são que o *site* malicioso deverá ser bloqueado pelo *web proxy* e que o PC1 deverá ser analisado pois provavelmente não tinha antivírus instalado ou estava desatualizado.

Salienta-se que o exemplo anterior é simplista e serve apenas para ilustrar as capacidades de um SIEM. O que se pretende concluir é que os *logs*, por si, raramente contêm a informação necessária para se compreender as implicações de um determinado evento no contexto da organização.

Por último, destaca-se que não é possível a uma

organização ter analistas de segurança que entendam a informação que é apresentada em *logs* nos mais diversos formatos. Uma das mais-valias dos SIEM é a sua capacidade de normalizar estes *logs*.

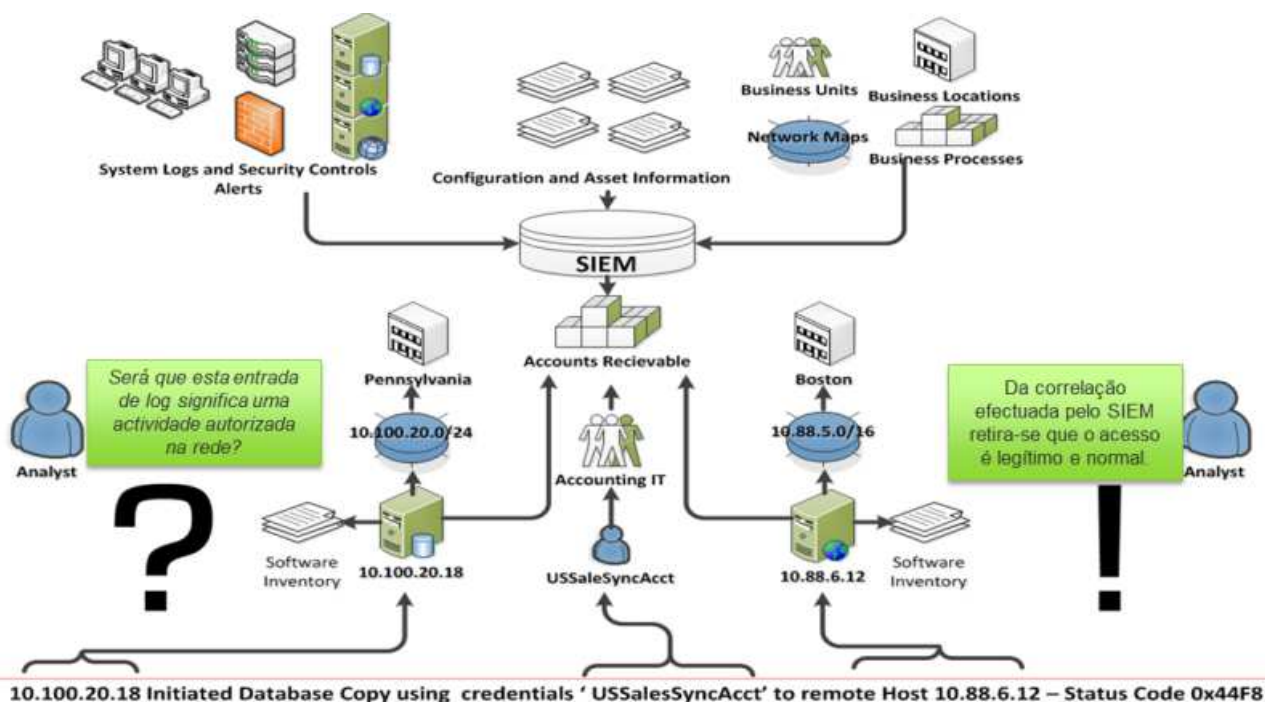
O Poder da Correlação

A correlação de eventos, de forma resumida, tem como objetivo principal gerar alarmes para responder às seguintes perguntas: “Quem está a atacar a organização?”; “De onde veio o ataque, como chegou onde chegou e o que pretende?”.

Poder-se-á pensar que os controlos implementados por soluções de perímetro como *firewall*, IDS/IPS e antivírus poderão ser a solução para responder a estas perguntas. No entanto, a maior parte das vezes a única informação que esses controlos fornecem são os eventos que detetaram num determinado momento e não o “antes e o depois”.

Atualmente os ataques bem-sucedidos aos SIC de uma organização raramente o aparentam ser. Se assim fosse, seria relativamente fácil automatizar os referidos sistemas de proteção sem sequer ser necessária a intervenção de um analista.

Idealmente, conforme apresentado na figura seguinte, todos os sistemas operativos, aplicações e



Correlação de eventos relativos ao acesso a uma base de dados por parte de um utilizador (Fonte: OSSIM)



equipamentos gerariam os seus *logs* em formatos compatíveis e suscetíveis de serem facilmente entendidos – na realidade tal não acontece.

Para que o SIEM possa correlacionar os eventos recebidos da rede é necessário normalizar os *logs*. Para tal, as soluções SIEM têm centenas de *plugins* desenvolvidos com o objetivo de receber os *logs* de fabricantes/sistemas diferentes e normalizá-los. Estes *plugins* são por norma ficheiros XML¹¹ que podem ser particularizados ou alterados pelo próprio analista caso este tenha necessidades muito específicas.

O passo seguinte é então a correlação dos eventos recebidos após a normalização dos *logs*. É nesta etapa que reside a mais-valia dos SIEM relativamente aos sistemas de análise dos *logs* dos IDS/IPS. O objetivo principal é analisar a multitude dos eventos recebidos de diferentes fontes e decidir, baseado em regras estabelecidas, se esses eventos deverão, ou não, originar um alarme.

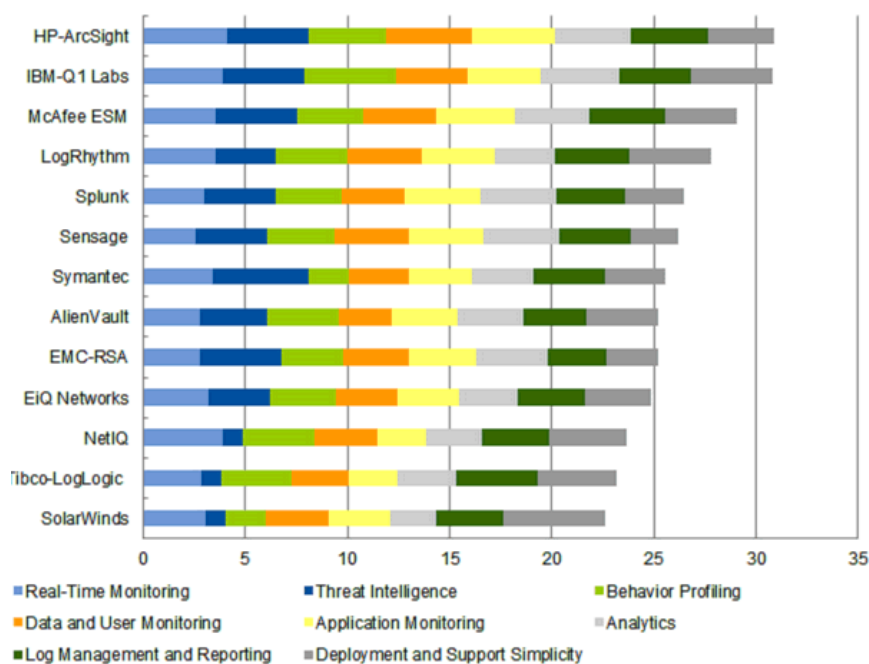
Esta característica dos SIEM tem a particularidade de, ao contrário dos IDS/IPS, não se basear apenas em assinaturas de ataques ou de *malware*. Assim, o SIEM poderá prevenir os denominados *zero day attacks*, avisar quanto a potenciais vulnerabilidades até aí desconhecidas e minimizar as *Advanced Persistent Threats* (APT)¹². Tal acontece pois o SIEM não se está a basear em assinaturas e/ou listas pré-definidas mas sim em regras e análise de padrões de comportamento que não são visíveis através dos *logs* gerados por aplicações ou equipamentos de forma isolada.

¹¹ Extensible Markup Language – formato de ficheiro que tem como objetivo padronizar um documento para que possa ser lido tanto por pessoas como interpretado por um programa.

¹² O objectivo de uma APT é o roubo de informação em oposição a causar danos nos sistemas de uma organização, que, por norma, possui informação de alto valor. Desta forma o APT pretende passar despercebido e ficar indetectável durante o maior tempo possível. Um dos vectores de ataque utilizados pela APT é a Engenharia Social.

Exemplo de um SIEM

Conforme apresentado seguidamente existem atualmente no mercado diversas soluções de SIEM com diferentes funcionalidades e capacidades. No entanto, conceptualmente, todas elas são semelhantes.



Análise de diversos produtos SIEM (Fonte: Gartner)

Apesar de sair fora do âmbito deste artigo a comparação de diferentes soluções, salienta-se que existem ou existiram no mercado outras soluções que se enquadram apenas no conceito de SIM (*Security Information Management*) ou SEM (*Security Event Management*), como por exemplo, o Cisco Security Monitoring, Analysis, and Response System (CS-MARS), atualmente descontinuado. Daí o facto de estas soluções não terem sido analisadas pelo estudo referenciado na figura anterior.

A empresa AlienVault foi uma das que surgiu mais cedo no mercado dos SIEM, por volta de 2003, e tem atualmente no seu portefólio o produto OSSIM (*Open Source Security Information Management*) que é gratuito e suportado por uma vasta comunidade de programadores e analistas de segurança. De seguida, apresenta-se uma breve descrição deste SIEM.



O OSSIM tem na sua base quatro componentes principais, conforme apresentado na figura seguinte: sensores, uma base de dados, *framework* e o servidor.

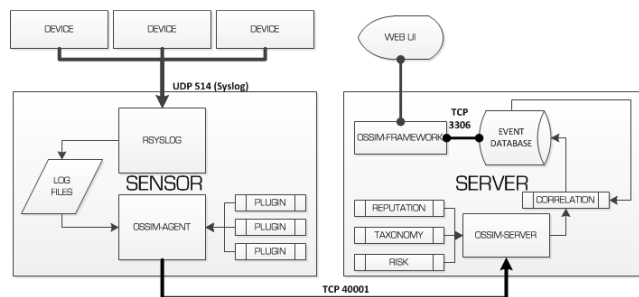


Diagrama lógico dos componentes do OSSIM (Fonte: OSSIM)

Os sensores, que poderá apenas ser um, são colocados ao longo da rede, geograficamente dispersos, e perto dos equipamentos de onde se pretende receber os *logs*. Os sensores podem ainda correr outro tipo de aplicações, como por exemplo para análise de tráfego e/ou vulnerabilidades (e.g. *snort* ou o *nessus*). Nos sensores é onde se encontram os *plugins* que permitirão normalizar os *logs* conforme apresentado anteriormente, e gerar eventos;

- A base de dados é o ponto central de recolha dos eventos oriundos dos diversos sensores tanto na fase de pré-correlação como na de pós-correlação;
- O servidor é o “cérebro” do OSSIM e irá executar a correlação dos eventos. Esta correlação tem por base *inputs* de diversas fontes. Além das vulnerabilidades e padrões de análise que lhe são conhecidos, o servidor irá basear-se também na reputação de cada endereço IP, no risco atribuído, por exemplo, a um segmento de rede (e.g. uma DMZ ou *DataCenter*) e na taxonomia, definida por defeito ou personalizada por um analista, dos tipos/classes de eventos (e.g. *logins*);
- A *framework* é o componente que permite apresentar os eventos recebidos, a correlação efetuada e os alarmes gerados após a correlação de uma forma gráfica ao analista, conforme

ilustrado nas duas figuras seguintes. Permite ainda gerir os diversos sensores, treinar o motor de correlação, categorizar o risco associado a cada equipamento ou serviço e, finalmente, elaborar relatórios para uma análise integrada das ameaças detetadas na rede como um todo.



Exemplo de uma aplicação SIEM denominada OSSIM (Fonte: OSSIM)

Displaying events 1-6 of 6 total

Signature	Total #	Sensor #	Src. Addr.	Dst. Addr.	Graph
Cisco-IPS: UDP eDonkey Activity	849(3%)	1	10	281	
Cisco-IPS: TCP SYN Host Sweep	31336(93%)	1	128	6228	
Cisco-IPS: BitTorrent Client Activity	10(0%)	1	1	10	
Cisco-IPS: IRC Server Connection	3(0%)	1	2	1	
Cisco-IPS: SQL Query in HTTP Request	4(0%)	1	1	1	
Cisco-IPS: IRC Channel Join	1555(4%)	1	4	3	

Exemplo de eventos recebido de IPS Cisco (Fonte: OSSIM)

Como nota final salienta-se que o OSSIM tem ainda a capacidade de verificar se os controlos determinados pelas normas ISO27001 e PCI DSS 2.0 estão a ser cumpridos. Esta funcionalidade é denominada por *Compliance Mapping*.

Conclusões

O conceito subjacente a um *Security Information and Event Management System* (SIEM) é que toda a informação produzida por diversos Sistemas de Informação e Comunicações em diferentes locais geográficos é centralizada num único ponto permitindo, assim, a deteção de ameaças baseada não só em assinaturas como em padrões e



tendências, ação que não é possível alcançar recorrendo a sistemas isolados.

O SIEM permite disponibilizar aos analistas de segurança informação oriunda de diversos serviços, aplicações e equipamentos sem, no entanto, existir a necessidade daqueles terem acesso a esses sistemas e sem terem que percorrer dezenas de logs diferentes.

A correlação de eventos é o motor de inteligência dos SIEM e poderá resumidamente caracterizar-se da seguinte forma:

- Compara eventos de múltiplas fontes (i.e. aplicações, serviços, equipamentos) de forma a monitorizar utilizadores, processos, recursos, aplicações e tráfego;
- Relaciona os eventos ao longo do tempo de forma a detetar sequências de atividades que normalmente não deveriam ocorrer;
- Treina o SIEM de forma a este perceber o que é ou não normal num sistema, permitindo-o detetar ataques que de outra forma não seriam detetados por sistemas isolados.

A qualidade do produto final retirado de um SIEM é, contudo, diretamente proporcional à qualidade e quantidade de informação que ele recebe (i.e. logs). No entanto, em organizações com diversos tipos de sistemas e com cada um a gerar o seu tipo de informação é, hoje em dia, fulcral ter-se um único ponto de recolha de informação e elaboração de relatórios onde se possa ter uma visão global e holística da Segurança dos SIC e, conseqüentemente, da segurança da informação da organização a que estes pertencem.

Bibliografia

[1] AccelOps, 2012. *Compliance Management and Compliance Automation – How and How Efficient*. [Online] Disponível em: <http://www.accelops.com/blog/?p=149> [Acedido em 5/8/2013].

[2] Ahrendt, M., 2012. *Customizing AlienVault's OSSIM Plugins*. [Online] Disponível em: <http://mikeahrendt.blogspot.pt/2012/08/customizing-alienvaults-ossim-plugins.html> [Acedido em 5/8/2013].

[3] AlienVault Corp, 2013. *AlienVault - Intrusion Detection Capabilities and Usage Overview*. [Online] Disponível em: <https://alienvault.bloomfire.com/> [Acedido em 5/8/2013].

[4] AlienVault Corp, 2013. *How Alienvault Components Communicate*. [Online] Disponível em: <https://alienvault.bloomfire.com/> [Acedido em 5/8/2013].

[5] AlienVault Corp, 2013. *Log Collection, from the device, to the screen*. [Online] Disponível em: <https://alienvault.bloomfire.com/> [Acedido em 05/8/2013].

[6] Kibirkstis, A., 2009. *What is the Role of a SIEM in Detecting Events of Interest?*. [Online] Disponível em: <http://www.sans.org/security-resources/idfaq/siem.php> [Acedido em 5/8/2013].

[7] Lane, A., 2010. *Understanding and Selecting SIEM/LM: Use Cases, Part 1*. [Online] Disponível em: <https://securosis.com/blog/understanding-and-selecting-siem-lm-use-cases-part-1> [Acedido em 5/8/2013].

[8] Levin, D., 2009. *The convergence of SIEM and log management*. [Online] Disponível em: <http://www.networkworld.com/news/tech/2009/03/1909-tech-update.html> [Acedido em 5/8/2013].

[9] Nicolett, M. & Kavanagh, K., 2013. *Critical Capabilities for Security Information and Event Management*. [Online] Disponível em: <http://www.gartner.com/> [Acedido em 05/8/2013].

[10] Unisys, 2012. *Security Operations Centers, Monitorização, arquivo e correlação de eventos de segurança*. [Online] Disponível em: http://www.unisys.com/unisys/inc/countrysites/pdf/PT_CLB_SOC.pdf [Acedido em 5/8/2013]



Tecnologia

Contributo da Análise Forense Digital para a capacidade de *Intelligence* do Exército



Nuno Goes

Cap Tm (Eng)

“Os modernos campos de batalha necessitam cada vez mais de informação de qualidade e em tempo oportuno, ... essenciais para o desfecho das operações e para a correta tomada de decisão por parte dos comandantes.”

Com a expansão da Internet à escala global, a eliminação das fronteiras gerou um grande problema para as instituições no combate ao crime, uma vez que potenciou a ocorrência de crimes eletrónicos onde a vítima e o criminoso estão em lugares geograficamente distintos, extravasando as fronteiras de soberania de um país, configurando-se a grande maioria das ocorrências como delitos internacionais.

Torna-se assim necessário e primordial para o sucesso da investigação e da missão, a troca de informações e provas eletrónicas entre as agências de investigação. Por se tratar de um fenómeno e uma necessidade muito recente, ainda não existem padrões internacionais para o tratamento desse tipo de prova que obtenha consenso entre as entidades a que cabe a investigação. Assim, o valor jurídico de uma prova eletrónica recolhida e manipulada, sem padrões pré-estabelecidos, pode ser contestada e frequentemente inviabiliza a investigação devido à nulidade das provas apresentadas.

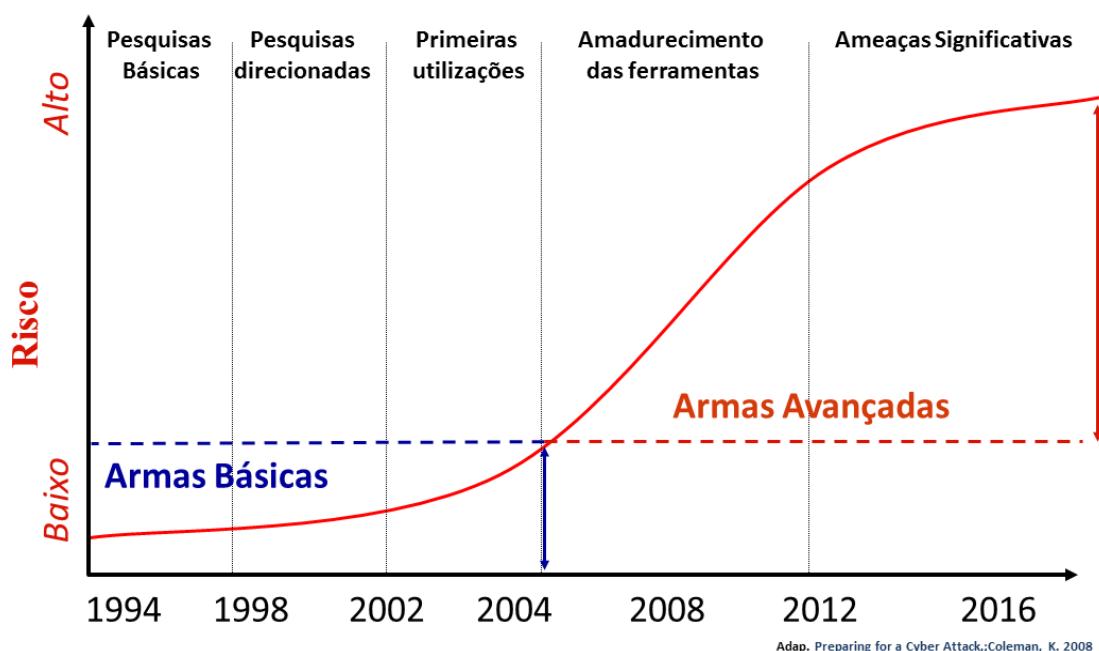
A ciência forense digital é um campo de pesquisa relativamente novo e em desenvolvimento, principalmente pela necessidade das instituições atuarem no combate ao crime informático. Em Portugal, existem muito poucos investigadores nesta área, estando o grupo dos que a podem praticar, para angariar prova passível de utilização em processo penal, habitualmente restrito aos investigadores da Secção de Investigação de Criminalidade Informática e Tecnológica da Polícia Judiciária (SICIT-PJ)¹³.

Hoje, a análise forense digital¹⁴ é considerada como ciência, sendo suportada com base numa metodologia, assente em observações, tese, investigação e testes com o único objetivo de mostrar a ligação entre os vestígios de um crime e aquele que os gerou. Edmund Locard¹⁵, notável investigador forense francês do século XIX e diretor do primeiro laboratório criminal, construído na cidade francesa de Lion, contribuiu para esta ciência com uma frase que nunca deixa de estar atual: “todo o contacto deixa vestígio”.

13 Conforme o constante do Art. 7.º (Competência da Polícia Judiciária em matéria de investigação criminal) da Lei n.º 49/2008 que aprova a Lei da Organização da Investigação Criminal

14 Análise forense digital é a aplicação de técnicas de investigação e análise para reunir e preservar as provas a partir de um dispositivo de computação particular, de uma forma a poder ser apresentado em tribunal de direito. Tem como objetivo a realização de uma investigação estruturada, mantendo uma cadeia de prova documentada para descobrir exatamente o que aconteceu num dispositivo de computação e quem foi o responsável pela ação ou evento. (Rouse, 2013)

15 A teoria de Locard exprime que “através do contacto entre dois itens, irá haver uma permuta. Basicamente a teoria de Locard, ou o princípio de Locard é aplicável nas cenas do crime, no qual o interveniente (ou intervenientes) da cena do crime entra em contacto com a própria cena onde o crime foi executado, trazendo algo para a cena do crime. Cada contacto deixa o seu rasto. Podem ser consultados mais dados em: http://pt.wikipedia.org/wiki/Teoria_de_Locard



Evolução do risco em função da ameaça ao longo do tempo

Segundo o Código Civil Português¹⁶, no disposto pelo artigo 388º, “a prova pericial tem por fim a percepção ou apreciação de factos por meio de peritos, quando sejam necessários conhecimentos especiais que os julgadores não possuem, ou quando os factos, relativos a pessoas, não devam ser objeto de inspeção judicial”. Segundo o que nos é apresentado, depressa se percebe que, no âmbito do crime informático há a necessidade de recorrer a peritos em ciência forense digital, devido à especificidade da matéria e aos requisitos técnicos necessários. A salvaguarda da cadeia de custódia, a integridade da prova, as técnicas de investigação entre outros temas na ciência forense digital ainda são assunto tabu para grande parte dos juristas, membros do Ministério Público, magistrados e para a Instituição Militar. Assim, sabendo que uma prova pericial eletrónica é passível de fraude ou manipulação se não for tratada ou recolhida segundo procedimentos e normas, facilmente se entende que esta pode ser objeto de deturpação ou invalidade jurídica, quebrando os aspetos éticos,

técnicos e legais. Qualquer falha na cadeia de prova compromete a utilização da mesma em tribunal.

A evolução da ameaça tecnológica

É indiscutível que a tecnologia é parte integrante do nosso dia-a-dia e que a Internet se tornou num instrumento indispensável, encurtando distâncias e acelerando a comunicação. Contudo, este avanço trouxe também o crescimento dos atos ilícitos e crimes de índole informática como as fraudes, roubo de *passwords*, violação dos direitos de autor, entre muitos outros. A própria instituição militar, apoiada cada vez mais em sistemas de informação e meios que potenciam a capacidade de comando e controlo e a superioridade de informação¹⁷ não fica à parte desta ameaça, sendo várias as nações que já criaram forças especiais para atuar neste campo, e usando

¹⁶ Disponível em: <http://www.homepagejuridica.net/attachments/article/784/C%C3%B3digo%20Civil%20outubro%202012.pdf>

¹⁷ Entende-se Superioridade de Informação como o grau de domínio no âmbito das informações que permitam a realização de operações sem oposição eficaz por parte do opositor (FAS, 2010) ou “a capacidade para pesquisar, processar e difundir um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade do adversário para fazer o mesmo” segundo o Concept for Future Joint Operations disponível em <http://www.dtic.mil/jv2010/cfjoprnr1.pdf>

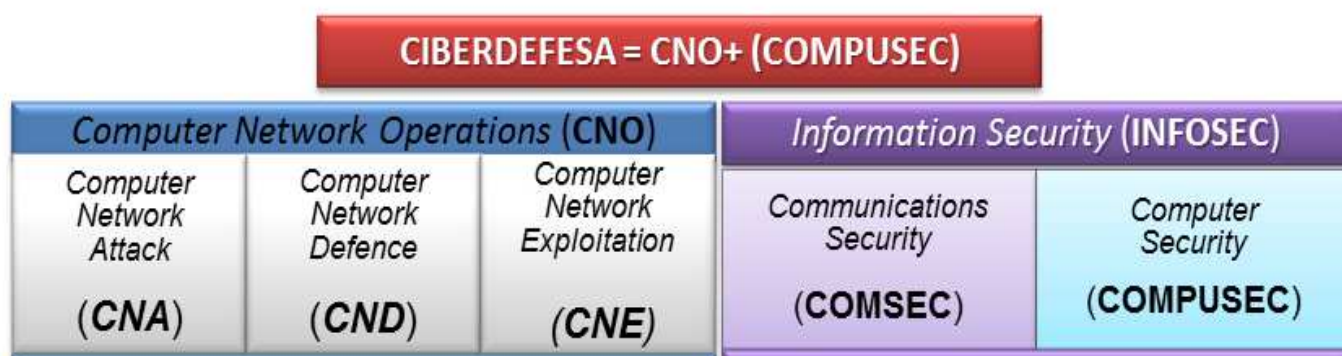


para esse efeito técnicas e meios eletrónicos para combater os seus adversários¹⁸.

Inicialmente, a ameaça era constituída por elementos que se iniciavam na descoberta de vulnerabilidades, demonstrando um grande amadorismo e poucos recursos, apresentado uma ameaça pequena que se traduzia num risco pouco significativo para as organizações. Com o passar dos tempos, os invasores foram ganhando conhecimentos, dedicando tempo e recursos, adquirindo tecnologia cada vez mais avançada, aumentando a eficácia e o impacto dos seus ataques. As organizações começam já a sofrer grandes perdas e percebem que têm que apostar na segurança dos seus ativos de informação aos seus mais variados níveis, investindo muitos recursos e tornando a segurança como um dos seus ativos vitais. Com o aumento da complexidade dos ataques houve, também, um aumento da consciencialização para a segurança da informação, o que levou a que a eficácia também diminuísse. A ilustração anterior pretende mostrar a evolução da ameaça, cada vez mais complexa, e o aumento do risco dos ativos da empresa ao longo do tempo.

meio informático. Consegue, através dos procedimentos adequados, recolher provas concretas como um ficheiro de imagem, uma agenda, uma mensagem de correio eletrónico, entre outros, sejam eles de um indivíduo que cometa uma ato ilícito ou de um membro duma força opositora que guarde nos seus dispositivos eletrónicos informações de grande valor e utilidade para aplicação tática. Para tal, o técnico que queira recolher as provas deve ter conhecimentos técnicos profundos sobre os sistemas que vai abordar, bem como conhecer as ferramentas adequadas para efetuar a aquisição e a análise tendo a noção global das implicações de todas as ações que vier a executar no sistema. Deve executar a perícia sem perturbar o sistema em análise para não inviabilizar a reconstrução dos dados. Deve garantir a integridade, a confidencialidade, autenticidade e o não repúdio das provas levantadas durante a análise para que possam, posteriormente, servir de prova num processo judicial ou legitimar uma intervenção militar.

Perante o cometimento de um ato ilícito, o lesado, visando a atribuição de uma responsabilidade (civil, criminal ou administrativa), a reparação ou



Componentes da Ciberdefesa

[adaptado. Cyber Defence Capability Framework Document (Ver.2 -28Feb11)]

A ciência forense digital visa suprir as necessidades no que se refere à manipulação de provas eletrónicas. É uma ciência que estuda a aquisição, preservação, recuperação e análise de dados em formato digital, armazenados em qualquer tipo de

retribuição devido a um ato ilícito sofrido, pode depender da manutenção de uma linha condutora, estabelecida entre a deteção e a recolha de informação pertinente (prova) e a sua apresentação num procedimento legal adequado à obtenção do resultado pretendido no âmbito de um processo

¹⁸ Como é o caso dos Estados Unidos da América, Alemanha, Inglaterra, Holanda, Noruega, China, etc.



judicial, num Tribunal Arbitral, ou ainda, num acordo entre partes.



Contributos da computação forense

No âmbito das Forças Armadas, as suas infraestruturas de informação são críticas e requerem uma análise e vigilância em tempo real de ciberataques ou tentativas de aquisição de informação, sem ter que retirar as máquinas do sistema em si nem desligar as mesmas para análise. Assim, é quase certo que o sistema de informação será o alvo principal do ataque e constituirá por si só a fonte primária de prova em conjunto com todos os equipamentos que sustentam a conectividade do sistema (ativos de rede como *routers* e *switchs*) permitindo reconstruir a ação temporal do ataque bem como o caminho percorrido, o *modus operandi* e a informação extraída ou que se tentou extrair. Permite também perceber como o sistema foi corrompido, que meios foram utilizados para o ciberataque e que vulnerabilidades foram exploradas bem como perceber quais os objetivos do atacante.

Esta avaliação é conseguida pela análise forense de dados digitais que desempenham um papel fundamental no processo de tomada de decisão dos militares no moderno campo de batalha, com o objetivo de perceber as intenções e a maneira de atuar do adversário, reduzindo continuamente a quantidade de tempo que leva a observar e

responder às ações do inimigo, de modo que a capacidade de reação do adversário é ultrapassado pelas nossas ações militares.

A deteção do ataque e a aquisição de prova em tempo útil permite identificar o alvo e ativar as medidas de ciberdefesa¹⁹, legitimando um possível ataque com a utilização da capacidade de *Computer Network Operations* (CNO), desde que se cumpram um conjunto de pressupostos, nomeadamente quando está em causa a integridade do próprio Estado.



Dadas as considerações acima expostas, poderemos considerar a aplicação militar da computação forense como a exploração e aplicação de métodos cientificamente comprovados para recolher, processar, interpretar e utilizar provas digitais para:

- Fornecer uma descrição conclusiva de todas as atividades do ciberataque com a finalidade de tipificar a ação sofrida e a sua reconstrução temporal bem como a restauração da informação e das infraestruturas que a suportam²⁰;
- Correlacionar, interpretar e prever as ações adversárias e seu impacto sobre as operações militares planeadas;
- Contribui para o ciclo de produção de informação;

19 Entende-se por ciberdefesa as “ações que combinam a garantia da informação, defesa das redes de computadores (incluindo ações de resposta) e proteção das infraestruturas críticas com recursos que permitem prevenir, detetar e, finalmente, responder à capacidade do adversário de negar ou manipular informações”. (Army, 2010)

20 Contribui diretamente para a capacidade de Disaster Recovery que contempla mecanismos avançados para recuperação das operações e serviços no caso ocorrência de acidentes graves de segurança ou desastres que possam afetar a infraestrutura tecnológica e os sistemas de informação, e consequentemente a segurança física e lógica da toda a informação armazenada, processada e em circulação na Rede.



- Verificar os dados digitais de forma adequada e conveniente, utilizando metodologias certificadas para a legitimação de uma possível ação militar ou de um processo de investigação criminal.

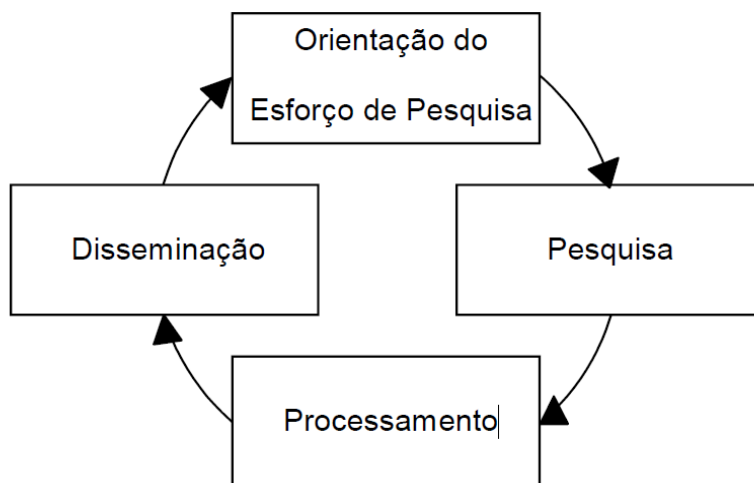
Toda a informação recolhida será de extrema importância para o comandante na tomada de decisão para que este perceba que tipo de ataque está a sofrer, que alvos ou ativos críticos estão em causa e que tipo de agressor tem pela frente. Todas estas variáveis têm que ser consideradas e podem influenciar muito o tipo de resposta, que meios serão usados e, acima de tudo, qual o enquadramento legal que pode, ou não, legitimar uma ação.

Ao nível das informações, é necessário perceber a cadeia de acontecimentos e o modelo de progressão do ciberataque para preparar a defesa mais adequada e evitar ações futuras. Esta aquisição de informação permite proteger as redes de futuros

informação é demorada e requer grande quantidade de recursos, não só materiais como humanos. Os suportes de informação têm cada vez mais capacidade de armazenamento e a celeridade de resposta exige que estejam a ser monitorizados em tempo real.

A evolução constante dos métodos utilizados para ataque, a proliferação de ferramentas grátis e a possibilidade de “comprar” um ataque a terceiros são desafios que até hoje não se concretizaram com grande impacto mas que, a acontecer, podem criar grandes perdas e, numa situação extrema, pôr em causa a soberania de um Estado.

Normalmente, a computação forense é mais utilizada em análise de factos já ocorridos, em que é analisada a informação deixada como prova para uma ação posterior. No âmbito militar exige-se a análise dos dados em tempo real nos sistemas de informação para que possa ser desencadeada uma



Ciclo da produção da informação

[adaptado. do PDE 2-00 Informações, Contra-Informação e Segurança]

ataques e o próprio desenvolvimento de aplicações e ferramentas²¹. Contudo, a análise deste tipo de

ação de resposta em tempo oportuno. Tendo em conta esta exigência, há a necessidade de mudar o paradigma do desenvolvimento de ferramentas forenses para a sua adaptação voltada à perspetiva das operações militares. Deve ter em conta a sua capacidade de aquisição de informação, principalmente na visualização de informação digital

21 Conforme requisito levantado pela União Europeia à Europol e ENISA no Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (pág. 14) (Consultado em: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf em 28/08/2013)



em tempo real, preservando a sua integridade, correlação de eventos multiplataforma, classificação da informação obtida e a restrição do acesso à mesma. Deve garantir a proteção dos dados bem como a capacidade de aquisição, cópia digital, extração e análise da informação e a apresentação de relatórios em tempo útil às operações.

A análise forense digital no campo de batalha

Hoje em dia já existem soluções portáteis para aquisição e análise de materiais a suportes de informação encontrados no terreno, independentemente do tipo de equipamento que contenha os dados²². As empresas têm em conta a necessidade da grande capacidade de armazenamento, a portabilidade, a robustez e a grande capacidade de processamento necessárias para efetuar a aquisição da imagem do dispositivo e efetuar uma primeira análise no local aos dados nele contido por imperativo da própria missão, bem como a capacidade de transporte pelo militar. Aqui, privilegia-se o tempo de acesso à informação e o cumprimento dos requisitos legais de preservação da prova. Normalmente estas soluções vêm munidas de um grande conjunto de interfaces, um computador robusto e todo o *software* necessário para efetuar a aquisição e análise dos dados recolhidos.



Colaboração entre entidades

Tendo em conta o interesse da superioridade de informação e a perspetiva da defesa da soberania nacional há a necessidade de trocar informação e conhecimentos aos nível dos procedimentos forenses digitais para normalização, apresentação da prova com valor jurídico e correlação de casos entre

os serviços de informações, os CERT's²³, os órgãos de investigação criminal e a instituição militar.

A diversidade de conhecimentos e técnicas utilizadas podem potenciar a capacidade de aquisição de informação e o *Site Exploitation*²⁴. Nos teatros de operações modernos a necessidade de ser capaz de recolher dados de todas as fontes utilizáveis tornou-se crítica. Na aquisição de informações de alvos encontrados, os operacionais e agentes por todo o mundo têm a necessidade de aprender novas capacidades que permitam a recolha de *Intelligence*²⁵ de muitas atividades nos vários âmbitos de investigação e que podem estar relacionadas.

Essas atividades incluem, entre outras, a capacidade de explorar e compreender²⁶:

- Documentos de pessoal (DOEX);
- Exploração de Comunicações Fixas / Móveis (Cellex);
- Exploração de meios eletrónicos (MEDEX);
- Materiais (Biometria).

A participação e a estreita colaboração entre entidades potenciam a capacidade de aquisição de

23 Abreviatura de Computer Emergency Readiness Team - que tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança colaborando numa rede de CERT's mundial. O português pode ser consultado em www.cert.pt.

24 Conjunto de atividades relacionadas dentro de um local sensível que explorem os documentos pessoais, dados eletrónicos e material capturado no local, que permitam neutralizar qualquer ameaça que o site/local revele através da análise dos dados aí encontrados (Joint Publication 3-31, 2010)

25 Intelligence ou informações (no âmbito militar) resulta de uma disciplina militar que explora uma série de recolhas e análises de abordagens a notícias e produzir informações para fornecer orientação e direção aos comandantes para apoio às suas decisões. É conseguido através de uma avaliação dos dados disponíveis a partir de uma ampla variedade de fontes, voltada para os requisitos da missão dos comandantes ou responder a perguntas específicas, como parte da atividade de planeamento operacional. As áreas de estudo podem incluir o ambiente operacional, as forças hostis, amigas e neutras, a população civil na área de operações, e outras áreas mais amplas de interesse. (Military Dictionary, 2008)

26 Segundo a Total Forensic Solutions em <http://tf-solution.com/capabilities/sensitive-site-exploitation/>, consultado em 28/08/13

22 Um dos exemplos disponibilizado pela DELL é o SPEKTOR <http://www.dell.com/learn/us/en/04/public~solutions~slg~en/document~spektor-competitive-comparison.pdf> consultado em 28/08/13



informações, contribuindo de forma crucial para a capacidade de *Intelligence*. Estas atividades são realizadas em todos os níveis, do nível tático ao estratégico, em tempo de paz, no período de transição para a guerra, e durante a própria guerra. São componentes essenciais no desenvolvimento da *Computer Network Exploitation* (CNE)²⁷ e caracteriza-se pelas ações de aquisição de informação através de redes informáticas que exploram os dados recolhidos a partir de sistemas de informação e redes do alvo ou inimigo. As CNE são usadas principalmente dentro das organizações militares. É um tipo de operação de cibersegurança, constituída por técnicas e processos que utilizam computadores ou redes de computadores para penetrar sistemas e redes alvo. Faz parte das *Computer Network Operations* (CNO)²⁸ e utiliza uma série de técnicas para a exploração, contribuindo para o ataque e defesa contra as entidades opositoras ou utilizadores mal-intencionados. A maioria dos governos mantém uma capacidade de produção de informações militares para recolha e análise de informações por unidades especializadas para todas as armas e serviços. Estas capacidades irão interagir com as capacidades dos serviços de informações civis para informar e potenciar a capacidade de tomar decisões em todo o espectro de atividades nos campos político e militar.

Contributo da Análise Forense Digital para a capacidade de Ciberdefesa

A análise forense digital, conjugada com um modelo de gestão para a Cibersegurança²⁹, fornece uma

abordagem lógica e compartimentada para avaliar o risco. Os procedimentos de garantia de tecnologia foram desenvolvidos como um dos principais componentes da análise forense digital e da metodologia de análise de segurança cibernética para fornecer a estrutura para o processo de avaliação de risco.

A execução e aplicação do modelo de gestão de segurança é realizada normalmente por um grupo multidisciplinar de profissionais de segurança tecnológica. O conjunto de relatórios de comunicação de comando começa a partir do auditor no terreno ou examinador, que apresenta os resultados ao escalão superior. Atua em vários domínios mas destaca-se nos domínios criminal, de informações, contra-informações, contra-terrorismo e de fraudes.

Conclusões

A análise forense digital apresenta-se como uma ferramenta essencial para a capacidade de *Intelligence* no domínio militar e civil, dando importantes contributos para o desenvolvimento das várias atividades desenvolvidas nos diversos âmbitos e produzindo informações que se podem considerar essenciais para o cumprimento das mais variadas missões. Requer elevados conhecimentos técnicos e meios tecnológicos para conseguir os seus objetivos. Os modernos campos de batalha necessitam cada vez mais de informação de qualidade e em tempo oportuno, fazendo com que a sua aquisição e correlação com informações já existentes sejam essenciais para o desfecho das operações e para a correta tomada de decisão por parte dos comandantes. É uma disciplina em franco desenvolvimento e uma ferramenta cada vez mais importante nas operações militares do futuro e que merece a devida importância por parte dos órgãos decisores.

27 Computer Network Exploitation (CNE) é uma técnica através da qual as redes de computadores são usados para infiltrar redes de computadores-alvo para extrair e recolher dados para as informações. Permite a exploração dos computadores individuais e redes de computadores de uma organização ou país externo, a fim de recolher todos os dados sensíveis ou confidenciais, que normalmente são ocultados e protegidos do público em geral. (AJP-3.10, 2009)

28 Computer Network Operations são ações deliberadas tomadas para alavancar e otimizar essas redes para melhorar potenciar o esforço humano ou de uma organização ou, no domínio da guerra, para ganhar superioridade de informação e negar o inimigo as vantagens que esta capacidade permite. (adap. de http://en.wikipedia.org/wiki/Computer_network_operations)

29 Entende-se Cibersegurança como o conjunto de ferramentas, políticas, conceitos de segurança, garantias de segurança, diretrizes, abordagens de gestão de risco, ações de formação, melhores práticas,

segurança e tecnologias que podem ser utilizadas para proteger o ambiente cibernético, a organização e os ativos dos utilizadores. Estes incluem dispositivos de computação ligados à rede, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações, bem como a totalidade das informações transmitida e/ou armazenadas no ambiente cibernético. (ITU, 2010)



Bibliografia

1. (CALL), C. f. (s.d.). TACTICAL SITE EXPLOITATION AND CACHE SEARCH OPERATIONS HANDBOOK. Obtido em 28 de Agosto de 2013, de The National Security Archive:
<http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB410/docs/Tactical%20Site%20Exploitation.pdf>
2. An Explanation of Computer Forensics. (2008). Obtido em 28 de Agosto de 2013, de Homeland Forensics:
<http://www.homelandforensics.com/Forensics/>
3. Army, U. S. (22 de Fevereiro de 2010). Cyberspace Operations Concept Capability Plan 2016-2028 (TRADOC Pamphlet 525-7-8). Obtido em 28 de Agosto de 2013, de Federation of American Scientists:
<https://www.fas.org/irp/doddir/army/pam525-7-8.pdf>
4. Computer Network Operations. (s.d.). Obtido em 28 de Agosto de 2013, de NSA - National Security Agency:
http://www.nsa.gov/careers/career_fields/netopps.shtml
5. Giordano, J., M. C. (2002). Cyber Forensics: A Military Operations Perspective. Obtido em 28 de Agosto de 2013, de Utica College:
<http://www.utica.edu/academic/institutes/eii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf>
6. ITU. (2010). Definition of Cybersecurity. Obtido em 28 de Agosto de 2013, de International Telecommunication Union:
<http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>
7. NATO. (2009). AJP-3.10 - ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS
8. NATO. (2012). National CyberSecurity Framework Manual. Obtido em 28 de Agosto de 2013, de CCDCOE - NATO Cooperative Cyber Defence:
<http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>
9. Rouse, M. (2013). Computer Forensics (Cyber Forensics). Obtido em 28 de Agosto de 2013, de TechTarget:
<http://searchsecurity.techtarget.com/definition/computer-forensics>
10. Spektor portable forensics kit. (s.d.). Obtido em 28 de Agosto de 2013, de Dell, Inc:
<http://www.dell.com/learn/us/en/04/public~solutions~slg~en/documents~spektor-competitive-comparison.pdf>
11. STAFF, J. C. (2010). Concept for Future Joint Operations. Obtido em 28 de Agosto de 2013, de DEFENSE TECHNICAL INFORMATION CENTER:
<http://www.dtic.mil/jv2010/cfjopr1.pdf>
12. Union, E. (s.d.). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Obtido em 28 de Agosto de 2013, de European External Action Service:
http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
13. Vacca, J. (2002). Computer Forensics: Computer Crime Scene Investigation. Boston: CHARLES RIVER MEDIA, INC.



ARTIGO DE OPINIÃO

Enquadramento Estratégico e Fundamentos para o desenvolvimento da Capacidade Nacional de Ciberdefesa



Reimão Teixeira

Maj Tm

“...o mundo acordou para uma nova realidade e para a imperiosa necessidade de implementar políticas de defesa e o levantamento de capacidades de ataque num quinto domínio operacional do campo de batalha, o ciberespaço”

O bloqueio ao normal funcionamento do governo e das instituições financeiras da Estónia em 2007 e da Geórgia em 2008 bem como os atrasos causados pelo vírus informático “Stuxnet” no programa nuclear iraniano no mesmo ano, como que “acordaram” o mundo para uma nova realidade e para a imperiosa necessidade de implementar políticas de defesa e o levantamento de capacidades de ataque num quinto domínio operacional do campo de batalha, o ciberespaço. As consequências destes ataques (os prejuízos financeiros, a desarticulação no funcionamento e consequente ameaça às soberanias dos países visados) aceleraram a criação/implementação de políticas, estratégias e estruturas que no geral implicaram um reforço dos meios e do pessoal necessário para as atingir.

Os Estados Unidos, país de referência sempre que analisamos tecnologia e a sua evolução, criaram em 2009 um Ciber Comando, enviando um claro sinal quanto ao elevado grau de importância dado ao assunto e desde a sua criação já quintuplicaram o seu efectivo. Em Maio de 2011 aprovaram a “*International Strategy for Cyberspace*” (US Government, 2011) e o seu Departamento de Defesa publicou em Julho do mesmo ano a “*Strategy for Operating in Cyberspace*” (US Department of Defense, 2011).



Em 2010, na cimeira de Lisboa, a Organização do Tratado do Atlântico Norte (OTAN) aprovou o novo conceito estratégico (NATO, 2010), em que é considerado como prioritário o levantamento de uma capacidade de ciberdefesa. Em Junho de 2011 é aprovado o “*NATO Policy on Cyber Defense*” (NATO, 2011).

A União Europeia (UE), como resposta ao problema identificado, aprovou em Fevereiro de 2013 dois documentos: “*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*” (CE, 2013) e “*Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*” (CE, 2013).



Portugal por seu turno aprovou um novo Conceito Estratégico de Defesa Nacional (Governo Português, 2013), onde podemos constatar que o ciberterrorismo e a cibercriminalidade são identificados como um dos riscos e ameaças ao ambiente de segurança global e nacional e nos apresenta como forma de resposta aos mesmos o desenvolvimento das capacidades militares necessárias à mitigação das consequências de ataques cibernéticos.

No mesmo diploma, é identificada a necessidade de avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados, sendo para tal definidas as seguintes linhas de ação prioritárias:

- Garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Protecção da Infra-estrutura de Informação Nacional (SPIIN);
- Definir uma Estratégia Nacional de Cibersegurança;
- Montar a estrutura responsável pela Cibersegurança, através da criação dos órgãos técnicos necessários;
- Sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática;
- Criar a capacidade de Ciberdefesa Nacional.

A implementação das orientações fundamentais da Política de Defesa Nacional, materializadas no novo Conceito Estratégico de Defesa Nacional, concretiza uma reforma estrutural da Defesa Nacional e das

Forças Armadas. Esta reforma estrutural, está vertida na Diretiva “Defesa 2020” (Ministério da Defesa Nacional, 2013), que tem como objectivo principal uma melhor utilização dos recursos existentes reconhecendo e atribuindo um elevado grau de prioridade ao levantamento de uma capacidade nacional de Ciberdefesa.

Num mundo cada vez mais dependente da ligação à rede e hiperconectado, em que tudo fica “à distância de um clique”, numa altura em que os riscos de ataques cibernéticos em grande escala são cada vez maiores e em que as expressões “ciberguerra” e “ciber 9/11” são usadas com cada vez maior frequência, a área ciber é, e será sem dúvida, a área de conhecimento com maior possibilidade de crescimento. A tarefa que se apresenta é essencialmente a de conseguir assegurar a identificação e mitigação das vulnerabilidades e ameaças em modo contínuo, de criar e manter um processo colaborativo para partilha de informação de forma a facilitar a transmissão de conhecimentos e facilitar a aprendizagem dos que connosco asseguram a Defesa Nacional.



O processo de desenvolvimento da capacidade de Ciberdefesa deve atender ao facto de as capacidades não serem criadas “por decreto”, a existência de uma estratégia/política/estrutura de ciberdefesa por si só não significa que a passemos a ter, mantendo assim uma visão o mais realista e coerente possível. As necessidades de formação serão muitas e o levantamento dessa capacidade na sua plenitude



demorará o seu tempo e implicará alterações nos conteúdos a ministrar em todos os níveis de formação por forma a garantir a sua edificação e continuidade. A eventual vinda da Escola de Comunicações e Sistemas de Informação da OTAN, atualmente residente em Latina-Itália, tem de ser encarada como um importante desafio, de enorme responsabilidade, para que Portugal se constitua como pólo de conhecimento e referência na área.

Por último importa realçar que na “Directiva 2020” apresenta-se como medida central: *“racionalizar a despesa militar, nomeadamente através da melhor articulação entre os ramos das Forças Armadas e uma maior eficiência na utilização de recursos”* o que conjugado com a adaptação da estrutura do EMGFA para: *“Criar um único serviço que coordene as comunicações e os sistemas de informação, em articulação com os ramos, procurando-se a sua centralização num único polo e a implementação de uma plataforma transversal de apoio à decisão, designadamente no que diz respeito às funções de comando, controlo e direção (NATO, 2011). O Centro de Ciberdefesa a criar deverá estar localizado junto deste serviço”*.

Os desafios são grandes, a Arma de Transmissões e o Exército têm demonstrado capacidade realizadora, facto que constitui um elemento fundamental para o sucesso num **futuro que... Começa agora**.



Bibliografia

CE. (7 de Fevereiro de 2013). Digital Agenda for Europe - European Commission. Obtido de <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>

Governo Português. (Março de 2013). Publicado Novo Conceito Estratégico de Defesa Nacional. Obtido de Governo de Portugal: http://www.portugal.gov.pt/media/909457/20130405_cedn_publicacao_oficial.pdf

Ministério da Defesa Nacional. (11 de Abril de 2013). RESOLUÇÃO DO CONSELHO DE MINISTROS, «DEFESA 2020». Obtido de Operacional: <http://www.operacional.pt/docs/Defesa%202020%20Resolu%C3%A7%C3%A3o%20Conselho%20Ministros.pdf>

NATO. (Novembro de 2010). NATO's New Strategic Concept. Obtido de NATO: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

NATO. (4 de Outubro de 2011). Cyberdefense PDF Library. Obtido de North Atlantic Treaty Organization: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf

US Department of Defense. (Julho de 2011). US Department of Defense. Obtido de defense.gov: <http://www.defense.gov/news/d20110714cyber.pdf>

US Government. (Maio de 2011). The Whitehouse Washington. Obtido de http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf



Regimento de Transmissões

Dia da Unidade

36 Anos ao serviço de Portugal



17 de Setembro de 2013

Powered by RT



Tecnologia

The National Cybersecurity Workforce Framework - USA / EUA



Costa Silva

Cap Tm (Eng)

“Foi identificado que a capacidade de preparar, educar, recrutar, treinar, desenvolver e manter trabalhadores altamente especializados em cibersegurança, seria vital à salvaguarda da sua informação, ...

Desde sempre os Estados Unidos da América (EUA) têm sido um alvo privilegiado da espionagem industrial e militar d

e outros países. Estas ações aumentaram exponencialmente com a evolução da Internet e devido ao facto de vivermos cada vez mais numa sociedade ligada em rede. Tendo por base este cenário foi decidida a criação de um Cibercomando, o que veio trazer uma nova dimensão às operações militares, garantindo a capacidade dos EUA efetuarem Operações Centradas em Rede (*Computer Network Operations – CNO*) à escala global.

Apesar deste facto os EUA vêem-se impotentes para deter os ataques de que são alvo diariamente, tendo constatado que a segurança de um país é feita por todos, garantindo nomeadamente a proteção das Infraestruturas Críticas, entidades empregadoras, universidades e todos os cidadãos de uma forma geral.

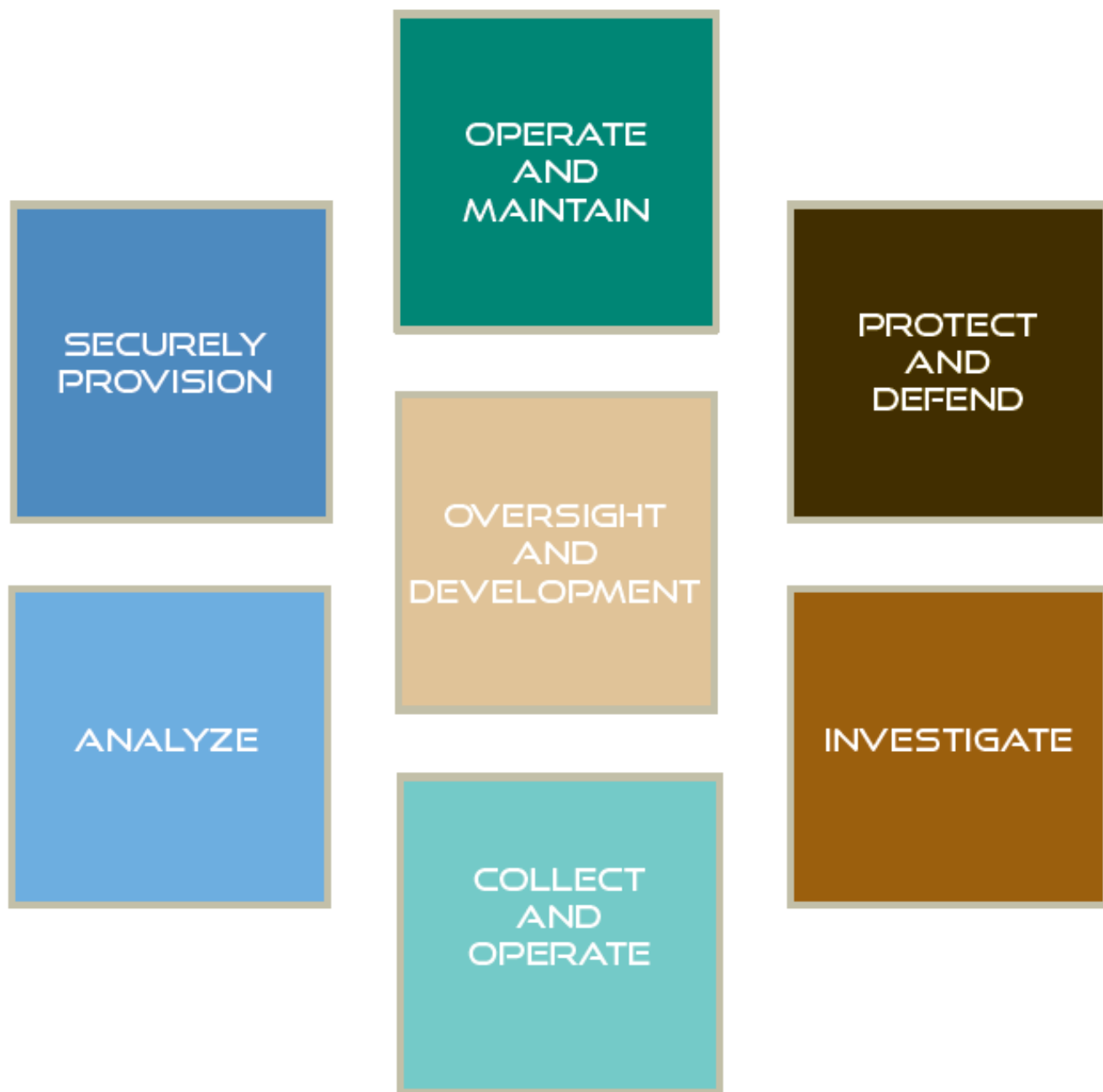
Assim foi feito um esforço para melhor compreender o problema e rapidamente se concluiu que existiam diversos problemas estruturais que deveriam ser resolvidos para que o país alcançasse a superioridade da informação.

Foi identificado que a capacidade de preparar, educar, recrutar, treinar, desenvolver e manter trabalhadores altamente especializados em cibersegurança, seria vital à salvaguarda da sua informação, prosperidade nacionais e à defesa das suas infraestruturas críticas.

Numa tentativa de perceber o motivo das vulnerabilidades existentes e a melhor forma de as colmatar, cedo se percebeu que existiam inúmeros conceitos com definições divergentes, bem como pouca consistência na forma como o trabalho nas áreas de cibersegurança é definido e descrito.

O facto de não existir uma linguagem comum para descrever e compreender o trabalho relacionado com cibersegurança dificulta o estabelecimento de padrões de capacidades, identificação de competências e garantia de que é ministrada a formação adequada aos profissionais. O facto de não existirem padrões bem definidos tem, de igual modo, levantado inúmeras dificuldades na resposta a incidentes e na tomada de medidas adequadas para fazer face ao riscos emergentes, ameaças, vulnerabilidades e à complexidade tecnológica que requer uma rápida aquisição de conhecimentos e competências.

Assim, foi entendido ser necessário estabelecer um léxico e taxonomia comuns, elaboração e validação de *job description*, elaboração de diversos outros *standards* e levantamento de requisitos.



Em 2010 o presidente Barack Obama estabeleceu a *National Initiative for Cybersecurity Education* (NICE), uma iniciativa nacional coordenada e com objetivo de aumentar a consciencialização para a segurança, a educação, o treino, e desenvolvimento profissional em segurança da informação.

Na sequência desta iniciativa, o *National Institute of Standards and Technology* (NIST) recebeu a tarefa de identificar uma *framework* para todos os trabalhadores ligados à cibersegurança, que fosse adaptável às necessidades das diversas instituições

nacionais americanas (*"The National Cybersecurity Workforce Framework"*).

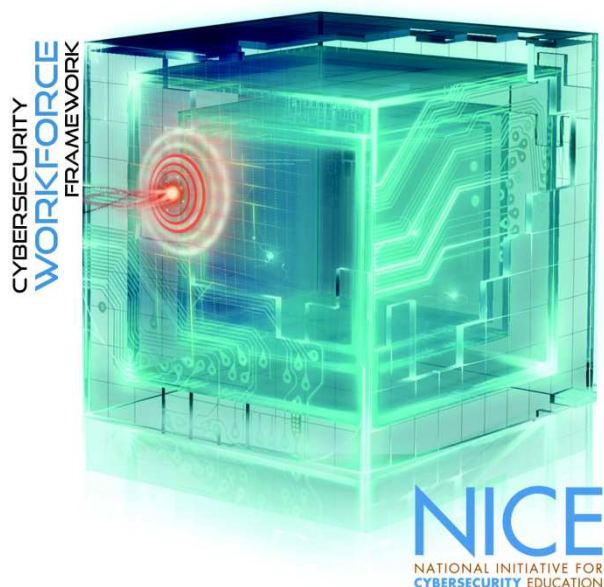
A Framework

O objetivo da *framework*, que se encontra ainda em *draft* final, é o de procurar desenvolver um melhor entendimento das funções dos elementos que trabalham em cibersegurança, de forma a dotar estes elementos com a formação e perícia necessárias ao desempenho das suas funções.

A *framework* identifica sete categorias de topo, que incluem mais de trinta áreas de especialização no



total. As categorias da “National Cybersecurity Workforce Framework” podem ser observadas na figura anterior (fonte: www.nist.gov).



As sete categorias da *framework* são:

• **Securely Provision (Planeamento / Provisão de Segurança)** – Área de especialização responsável por conceptualizar, projetar, e ³⁰construir sistemas de *Information Technology* (IT) seguros. Esta categoria inclui ainda a *Information Assurance* (IA), desenvolvimento de aplicações seguindo normas de segurança e boas práticas, entre outras;

• **Operate and Maintain (Operar e Manter)** – Área de especialização responsável por fornecer apoio, administração e a necessária manutenção, de forma a garantir um desempenho e segurança efetivo e eficaz nos sistemas de IT. Esta categoria inclui ainda a Gestão do Conhecimento e a manutenção dos equipamentos de segurança e das redes;

• **Protect and Defend (Proteger e Defender)** – Área de especialização responsável pela identificação, análise e mitigação de ameaças aos sistemas ou redes, e resposta a incidentes informáticos (*Computer Incident Response Capability* - CIRP). Estas especialidades trabalham em estreita

cooperação com os fabricantes de soluções de segurança;

• **Investigate** (Investigação) – Esta categoria engloba a área de especialização responsável pela investigação de eventos de segurança ou crimes que utilizem ou ocorram em redes ou sistemas de IT, bem como a recolha de prova digital e análise forense;

• **Collect and Operate** (Recolha e Operação) – Área de especialização responsável pela negação, condução de operações de decepção e recolha de informação cibernética que possa ser utilizada pelos serviços de informações;

• **Analyze** (Análise) – Esta categoria engloba a área de especialização responsável pela revisão e avaliação de informação recebida referente à cibersegurança, de forma a determinar a sua utilidade para os serviços de informações;

• **Oversight and Development** (Supervisão e Desenvolvimento) – Engloba a área de especialização que fornece liderança, gestão, direção e/ou desenvolvimento e aconselhamento jurídico, que permite que os indivíduos e organizações possam efetivamente realizar o seu trabalho de cibersegurança. Esta categoria é ainda responsável pela criação e manutenção de políticas de segurança e pela supervisão e coordenação das categorias anteriormente referidas.

A *framework*, disponível no portal do NIST em www.nist.gov, fornece ainda um conjunto de tarefas, funções, conhecimento e competências para cada uma das áreas de especialidade de cinco das categorias referidas. Ficam de fora as áreas mais ligadas às informações, por serem matéria mais sensível.

É ainda considerado fundamental que se utilizem as definições e designações referidas na *framework*, apesar de esta ser flexível e ter sido desenvolvida para ser adaptada às estruturas das diversas organizações. O objetivo é que se descreva as

³⁰ Responsável por alguns aspetos do desenvolvimento de sistemas.



tarefas, requisitos e competências utilizando um léxico comum.

A *framework* dá ainda indicações de que após a conclusão do processo de normalização, as organizações dever-se-ão empenhar em quatro grandes áreas fundamentais à cibersegurança nacional:

- **Recolha e análise de dados:** Recolha de informação junto dos elementos que dão formação ou trabalham em cibersegurança, de forma a compreender as capacidades, necessidades e vulnerabilidades;

- **Recrutamento e Treino:** Incentivar a contratação e permanência de profissionais altamente competentes e com elevada capacidade de adaptação;

- **Educar, Treinar e Desenvolver:** Aumentar o número de trabalhadores ligados à cibersegurança, bem como a sua formação e experiência. A educação em Segurança da Informação e ciberdefesa deve ser alargada a todos;

- **Compromisso:** Educar e motivar os elementos que desempenhem funções de cibersegurança, bem como todos os restantes trabalhadores (e população) de forma a criar uma cultura de segurança nacional que permita reforçar a defesas dos sistemas de informação nacionais.

Conclusões

A *framework* apresentada é um excelente exemplo do que é necessário fazer a nível nacional, no âmbito militar e civil, ao nível de competências e das tarefas num contexto integrado de cibersegurança.

Como seria de esperar, alguns pontos da *framework* já são utilizados pelo Exército Português que foi, a nível nacional, uma das primeiras Instituições a dar o exemplo, com a criação de um Núcleo e Módulo Tático de CIRC.

Dada a crescente importância da Segurança da Informação para a nossa sociedade, seria importante que fosse criado rapidamente um Centro Nacional de Cibersegurança e que todas as organizações nacionais trabalhassem cooperativamente. Só desta forma é possível dar uma resposta eficaz e necessária para fazer face a ameaças globais cada vez mais organizadas.

Bibliografia

http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf (Consultado em: 31 de Julho de 2013)





História

Comunicações HF Com Antenas NVIS

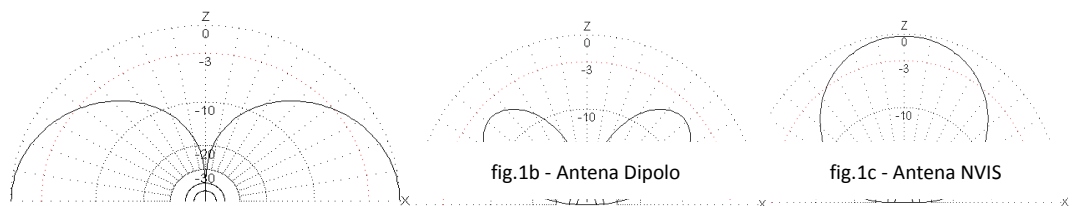
Rodrigo Leitão

TCor Tm (Eng) Ref

“O HF é ainda o meio que garante a sobrevivência das comunicações em situações em que os outros meios foram desativados ou bloqueados ...”

A primeira questão técnica com que me confrontei durante a comissão no Agrupamento de Transmissões de Angola (ATMA), de 1969 a 1973, foi a dificuldade em estabelecer ligações rádio em HF entre o Comando das unidades e os seus grupos operacionais.

Ou seja, cobrir distâncias de 0 a 200 Km sem qualquer zona de silêncio (*skip zone*) e em todas as direções (omnidirecional). O equipamento rádio era o Racal TR-28 (com 25W pep) que utilizava três tipos de antenas, conforme o tipo de instalação: vertical (*whip*), filar do tipo *longwire* e o dipolo G5RV. Após várias tentativas frustradas encontrei finalmente a solução no “*Radio Amateur’s Handbook*” (RAH). A sigla G5RV é o indicativo do rádio amador que a desenvolveu e que se baseia no princípio que a radiação dum dipolo colocado a uma altura abaixo de 1/8 do comprimento de onda tem um diagrama omnidirecional em que máxima radiação é vertical com incidência a 90 graus (Fig.1), e que sendo alimentado por uma linha não balanceada, mas não coaxial, há uma parte da radiação que é equivalente a uma antena vertical.



Numa das primeiras deslocações ao Norte de Angola, uma zona muito arborizada, tive contacto com o Comandante de um Pelotão de Caçadores, que me disse não ter qualquer dificuldade nas ligações com os seus grupos operacionais e/ou com o Posto de Comando. Utilizava a antena de fio que colocava estendida sobre o solo e a ligação era sempre de boa qualidade sem zonas de silêncio (*skip zone*). Ora isto significava que a antena de fio sobre o solo se comportava como uma antena NVIS.

Fiz então vários testes experimentais com muito bons resultados com antenas em modo de propagação NVIS (“*Near Vertical Incidence Skywave*”) calculadas com base nas fórmulas do “RAH”. Foram então produzidas pela CRM /ATMA antenas G5RV para instalações fixas e otimizadas para a gama de frequências atribuídas às unidades a que foram distribuídas tendo o problema ficado resolvido.



Alguns anos mais tarde li um artigo na revista SIGNAL escrito por um Coronel de Transmissões do Exército dos EUA que relatava situações semelhantes ocorridas no Vietname e que também tinham sido solucionadas com as antenas NVIS. Um dos casos descritos de antena com radiação NVIS era a antena vertical da viatura colocada paralela ao solo. Para tal mandou instalar na base da antena das viaturas um adaptador para esse fim, conforme

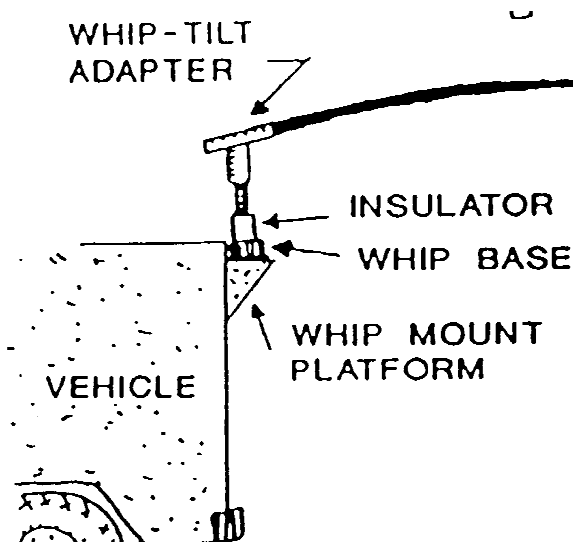


figura seguinte.

O que é a propagação ionosférica por NVIS?

É uma propagação em que a maior intensidade do campo elétrico radiado é na direção vertical.

O modo de propagação rádio NVIS permite estabelecer comunicações radioelétricas, via ionosfera, para lugares situados por detrás de obstáculos naturais ou artificiais, num raio superior a 400Km. Consegue-se eliminar as zonas de sombra (*skip zone*) ao selecionar uma frequência apropriada (situada abaixo da frequência crítica de reflexão) que impõe à antena dipolo ou monopolo um elevado ângulo de elevação entre 90º a 50º (efeito de “chapéu de chuva” ou “repuxo”)³¹.

³¹ Existem uma grande diversidade de antenas com que se pode obter uma propagação NVIS, sendo as mais utilizadas a Dipolo, o V invertido, a antena filar (longwire) e a antena de Loop. O diagrama de radiação

A reflexão ionosférica por efeito de NVIS não ocorre em qualquer frequência. Só se obtém com sucesso o efeito NVIS sabendo selecionar, ou descobrir (por tentativas), uma frequência que seja refletida pela ionosfera quando o ângulo de radiação é próximo da vertical. Estas frequências estão normalmente na gama de 2 a 10MHz.

A solução está em selecionar uma frequência que, naquele momento, esteja abaixo da frequência crítica de reflexão (a frequência mais alta refletida pela camada F com um ângulo de incidência de 90 graus) mas não abaixo da frequência crítica das camadas D e/ou E, para que estas não provoquem bloqueios. Atualmente a seleção da frequência está simplificada pois existem na internet *sites* (<http://nvis-tuga.blogspot.com>) que dão informação para cada local do Planeta e a qualquer hora da faixa de frequências entre a crítica das camadas D e E, e a crítica da camada F.

As antenas que no início mencionei são todas da classe das “Antenas de Campo Elétrico” (dipolos e monopolos), mas existe outra classe de antenas: as Antenas Magnéticas ou “LOOP ANTENNA” (Antena em Espiral). A primeira antena na história da Física, e da técnica rádio, foi a antena magnética que permitiu a HERTZ detetar que as faíscas eram transmitidas pelo espaço para uma pequena espiral a alguns centímetros de distância.

Esta antena, apesar de criar um diagrama de radiação idêntico ao de uma Antena de Campo Elétrico, tem “linhas de força” que começam por ser magnéticas e não elétricas.

A antena pode ter várias formas físicas: Quadrada, Losango, Triangular e Circular (Espiral) sendo o diagrama de radiação dependente da posição:

- Na posição horizontal a antena é omnidirecional e semelhante à antena

destas antenas depende do efeito refletor da superfície terrestre de forma semelhante ao efeito da parábola duma antena de micro-ondas. Qualquer antena de polarização elétrica horizontal (p.ex. o Dipolo) colocada a uma altura em relação ao solo inferior a 1/8 do comprimento de onda da frequência de trabalho tem um diagrama de radiação tipo NVIS.



vertical e diferente do dipolo que é bidirecional;

- Na posição vertical o diagrama de radiação é semelhante ao dipolo que também depende da altura em relação ao solo. Isto é, a uma altura abaixo 0,25 a 0,1 do comprimento de onda comporta-se como uma antena NVIS.

Considerando a banda dos 2 a 10 MHz o diâmetro de uma antena circular poderá ter 80cm mas com 150cm já tem uma eficiência e um ganho superior ao dipolo. Com estas dimensões é simples montar a antena em edifícios ou em espaços (parques, arruamentos, etc.) de maneira semelhante à montagem de antenas de televisão, conforme exemplos.

Estes tipos de antenas são ressonantes, e como tal necessitam de funcionarem em conjunto com uma unidade de sintonia de antena, mas têm a vantagem de se comportarem como um filtro seletivo reduzindo os efeitos de saturação e de produtos de intermodulação provocados por canais adjacentes. Uma outra vantagem da antena magnética resulta da insensibilidade a campos elétricos, como por exemplo os existentes em centros urbanos, provocados pelas instalações elétricas ou cabos de energia.



Para quê o emprego das faixas de HF nos nossos dias?

Apesar das novas técnicas de transmissão rádio o HF ainda é atualmente um meio de comunicação de grande importância em situações operacionais como aconteceu em Angola e Moçambique nas operações de paz UNAVEM e ONUMOZ, ou em outros teatros de operações onde existem forças nacionais

destacadas (FND), isto é, vastas áreas com intervenções operacionais muito dispersas. Também nos casos em que é complicado o recurso ao VHF por implicar a utilização de muitos repetidores ou por não ser possível a sua montagem para conseguir fazer a cobertura do TO. Estão nesta situação, por exemplo, nos Açores na ligação entre as ilhas, na

Madeira e Trás-os-Montes resultado do terreno muito acidentado com muitas zonas de sombra para o VHF. As bandas HF têm sido proteladas, em consequência da aparente complexidade em operar e estruturar as redes e quando confrontadas com as novas técnicas de transmissão no VHF, UHF, SHF, mas são atualmente excelentes meios de comunicações de voz e dados, resultado duma significativa evolução tecnológica nos últimos 15 a 20 anos nomeadamente na:

- seleção automática da frequência ótima (ALE);
- transmissão de dados a velocidades 100 vezes, ou mais, superior às dos anos 70;
- correção automática dos dados;
- transmissão em TCP/IP;
- sintonia automática da antena;
- COMSEC integrado;



- transmissão de dados a partir dum PC de mão (em vez dum teleimpressor);
- utilização de sintetizadores de frequência (em vez de cristais);
- processamento digital dos sinais (sinal com melhor qualidade na transmissão).

Conclusão

Atualmente, instalar e operar um posto rádio na faixa de HF por uma secção de transmissões é relativamente simples, mas não dispensa um treino continuado nas mais diversas situações operacionais.

O equipamento em uso no Exército para comunicações em HF em instalação *manpack* é o PRC 525 que tem integrado todos os módulos necessários para transmissão de voz e dados incluindo o COMSEC e o ALE. Com 20W é possível fazer a cobertura de todo o território continental em HF, e associado ao amplificador de 150W, em instalações transportáveis ou fixas, a área de cobertura estende-se às regiões autónomas e a todo o espaço europeu

O HF é ainda o meio que garante a sobrevivência das comunicações em situações em que os outros meios foram desativados ou bloqueados (calamidades, catástrofe, etc.), e, comparativamente com as comunicações via satélite, são mais económicas para estabelecer o *rear link* da FND com o Comando Operacional sedado em Lisboa.

Contudo há necessidade de treino permanente. Uma hipótese para assegurar no Exército esse treino, seria a criação duma rede entre as unidades equipadas com PRC525 tendo como posto diretor o Regimento de Transmissões ou o CFT, onde estão instalados sistemas fixos de comunicações em HF. Esta rede teria duas explorações diárias (de manhã e de tarde) com troca de mensagens numa rede rádio intranet.



Bibliografia

<http://www.qsl.net/w/wb5ude/nvis/>

<http://mysite.verizon.net/ka1fsb/loopants.html>

<http://www.dxzone.com/cgi-bin/dir/jump2.cgi?ID=21586>

<http://www.dxzone.com/cgi-bin/dir/jump2.cgi?ID=13330>



História

SITEP – Fibra Ótica



Cruz Fernandes

Cor Tm (Eng) Ref

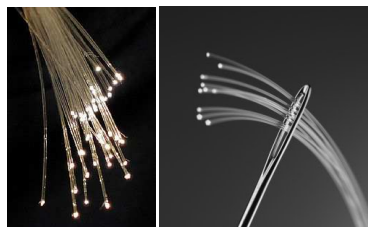
“As fibras óticas são largamente usadas em comunicações porque permitem a transmissão a longas distâncias com maiores larguras de banda do que outros meios de comunicação ...

Uma fibra ótica é uma fibra flexível e transparente feita de vidro ou de plástico, ligeiramente mais fina do que um cabelo humano. Ela funciona como um guia de ondas ou tubo de luz para transmitir luz entre os dois extremos da fibra.

As fibras óticas são largamente usadas em comunicações porque permitem a transmissão a longas distâncias com maiores larguras de banda do que outros meios de comunicação. As fibras são usadas em vez de fios metálicos por que os sinais viajam ao longo delas com menos perdas e são imunes às interferências eletromagnéticas. As fibras óticas tipicamente incluem um núcleo transparente envolvido por um material de revestimento transparente também mas com menor índice de refração. A luz é assim conservada no núcleo pela reflexão total interna. É isto que faz que a fibra seja uma guia de onda.

Fibras multimodo e fibras monomodo

As fibras que suportam muitos percursos de propagação ou modos transversos são chamadas fibras multimodo (MMF). Aquelas que apenas suportam um único modo são chamadas fibras mono modo (MNF). As fibras óticas desenhadas para transportar apenas um raio de luz são fibras monomodo. Os modos têm soluções dadas pelas equações de Helmholtz para as ondas, que são obtidas das equações de Maxwell combinadas com as condições locais. Os Modos definem as maneiras como a onda viaja no espaço, ou seja, como a onda se distribui no interior da fibra. As ondas podem ter o mesmo modo mas diferentes frequências. É este o caso que se verifica nas fibras monomodo, onde podem coexistir ondas com diferentes frequências mas com o mesmo modo, o que significa que elas são distribuídas no espaço de igual maneira e isto dá-nos um único raio de luz. As fibras multimodo têm um núcleo com maior diâmetro e são usadas para comunicações de curta distância e para aplicações onde seja de considerar a potência a transmitir. As fibras monomodo são usadas para distâncias superiores a 1050 metros.



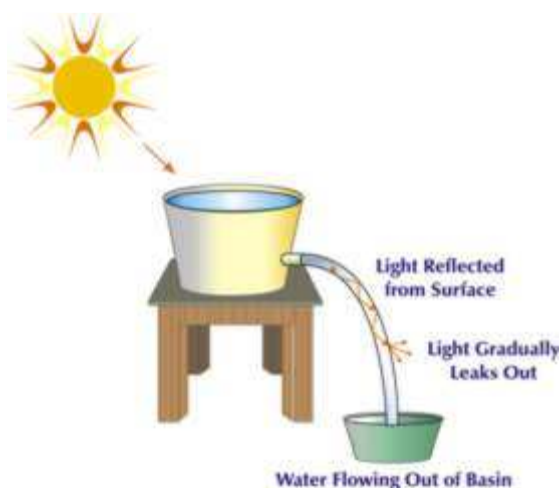
Fazer emendas em fibras óticas é mais complexo do que fazê-las em cabos de cobre. As pontas das fibras têm de ser cuidadosamente cortados, alinhadas e unidas ou mecanicamente ou fundindo-as com calor.



História

Guiar a luz por reflexão, princípio que torna as fibras óticas possíveis, foi pela primeira vez demonstrado por Daniel Colladon e Jacques Babinet em Paris, por volta de 1840. John Tyndall incluiu a demonstração desta possibilidade nas suas leituras públicas doze anos depois. Tyndall também escreveu acerca da propriedade da reflexão interna total, cerca de 1870: “Quando a luz passa do ar para a água, o raio refletido aproxima-se da perpendicular. Quando o raio passa da água para o ar, o raio refletido afasta-se da perpendicular. Se o ângulo que o raio dentro de água faz com a perpendicular à superfície for maior do que 48° , o raio refletido não sai da água. Será totalmente refletido à superfície”.

Para o vidro, o ângulo de reflexão total é de $38^\circ 41'$.



“fonte de luz” ou “tubo de luz” de Tyndall

O primeiro sistema de transmissão por fibra ótica foi demonstrado pelo físico germânico Manfred Borner nos *Telefunken Research Labs*, em Ulm, em 1965, a que se seguiu a primeira patente nesta tecnologia em 1966. Charles K. Kao e George Hockham da *Standard Telephone and Cables* foram os primeiros a promover a ideia de que a atenuação das transmissões por fibra poderia descer abaixo de 20db/km, tornando a fibra um meio de comunicação. E asseveraram que as atenuações eram devidas a impurezas, que podiam ser removidas, bem como a efeitos físicos como o

scattering (dispersão). Teorizaram os trabalhos para reduzir perdas nas fibras óticas e propuseram os materiais corretos a serem usados no fabrico de fibra: vidro de sílica com elevada pureza.

A NASA usou fibras de vidro nas câmaras de televisão que enviou à Lua. Nesta altura o uso de fibra em câmaras era *CONFIDENTIAL* e só pessoas credenciadas eram autorizadas a manejá-las.

Cientistas da *Corning Incorporated* baixaram, em 1970, a barreira de atenuação de 20db/km e demonstraram que uma fibra de vidro de sílica dopada com titânio tinha uma atenuação de 17db/km. Alguns anos mais tarde produziram uma fibra com uma atenuação de 4db/km, usando dióxido de germânio como dopante do núcleo.

A atenuação em cabos óticos é hoje de longe inferior à dos cabos elétricos, estabelecendo-se as distâncias entre repetidores de 70 a 150 km.

O amplificador de fibra ótica dopada com érbio que reduz o custo dos sistemas de fibra de longa distância pela redução ou eliminação dos repetidores ótico-elétrico-óticos foi desenvolvido por David N. Payne e por Emmanuel Desurvire, em 1986.

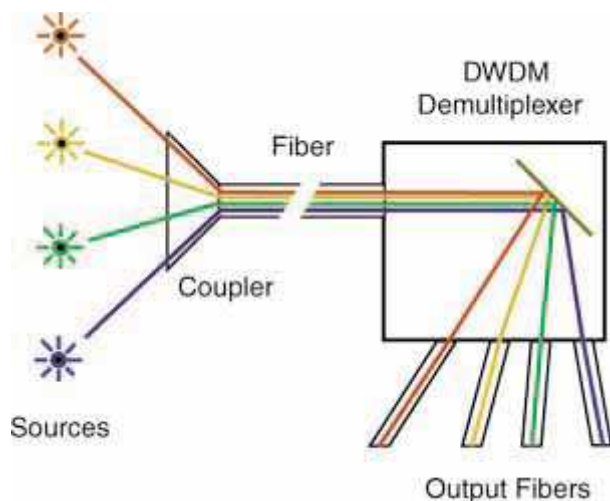
As modernas e robustas fibras óticas atuais usam vidro tanto para o núcleo como para a bainha.

Aplicações

A fibra ótica tem múltiplas aplicações mas a ênfase aqui é para redes de telecomunicações e de computadores. A fibra é especialmente vantajosa para comunicações a longa distância porque a luz propaga-se na fibra com pequena atenuação, se comparada com os cabos elétricos. Isto permite o uso de um número reduzido de repetidores cobrindo longas distâncias. Adicionalmente permite bit rates por canal de 111Gbits, segundo os NTT.

Cada fibra pode transportar vários canais (até oito) independentes, usando, cada um deles, um comprimento de onda de luz diferente (WDM –

Wavelength-division multiplexing). O recorde atingido até hoje pertence à *Bell Labs* de França, e consiste em 155 canais, cada um transportando 100Gbits num percurso de 700km de fibra.



Princípio do WDM

Importância da fibra ótica

A seguir apresenta-se o trabalho que justifica a necessidade de emprego da fibra ótica no SITEP e no PTAP que vem concretizar a introdução de uma nova tecnologia nas comunicações de Exército. Para avaliar a importância da ótica na vida do homem basta dizer que quase 100% da informação que este obtém a recebe pelo canal visual. Desde os primórdios da História e talvez já na pré-história que o homem transmite informação por meios visuais, tendo descoberto sucessivos meios de o fazer. Porém, só em 1970 é que surgiu a primeira linha de transmissão ótica. A partir daí produziram-se vidros de elevada pureza que permitiram a transmissão de luz com baixa atenuação. A utilização de fibras óticas em comunicações telefónicas envolve os seguintes passos:

- Conversão do sinal acústico em elétrico;
- Conversão do sinal elétrico em sinal luminoso;
- Conversão do sinal luminoso em sinal elétrico;

- Conversão do sinal elétrico em sinal acústico.

Apesar das transformações que o sinal recebe com o uso da fibra ótica, as fibras têm características que as elegem como preferenciais porque são competitivas quando se pretende:

- Imunidade ao ruído eletromagnético;
- Grande largura de banda;
- Baixa taxa de erros;
- Atenuações reduzidas;
- Custo sucessivamente mais baixo, ao contrário dos cabos convencionais;
- Baixo peso e pequeno diâmetro;
- Segurança nas comunicações (não há escutas);
- Isolamento total (não há fugas para a terra).

Assim as fibras óticas são o meio mais económico e eficaz para comunicações quer de longa quer de curta distância.

Quando se instalou a primeira fibra para o Exército o custo do cabo ótico ainda não era competitivo com os meios tradicionais, mas as restantes qualidades, nomeadamente a capacidade de transmissão digital tornou a escolha incontornável.

Escolha das Fibras e dos cabos de fibra ótica

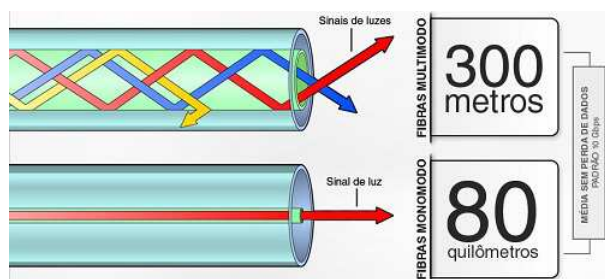
As fibras óticas, à data da sua introdução no Exército, agrupavam-se em duas categorias, segundo o modo de propagação:

- Fibras monomodo (MMF);
- Fibras multimodo (MMF). Estas subdividiem-se em fibras de índice de grau e fibras de índice gradual.

Fibras monomodo (MMF)



As fibras monomodo obtêm-se por redução do diâmetro do núcleo (1 a 5 micrones) e da abertura numérica ou ainda pela redução de ambos. A abertura numérica mede-se pelo seno do ângulo de incidência da luz de entrada na fibra.



Fibras Óticas Monomodo e Multimodo

As fibras monomodo introduzem menor distorção, possibilitam maior largura de banda e tem maior alcance entre repetidores. O facto de o seu núcleo ser extremamente fino coloca problemas, pois capta pouca luz da fonte luminosa de alimentação do sinal e sendo o ângulo da entrada do sinal luminoso, muito pequeno, resultam exigências muito apertadas quanto ao envio de luz para a fibra e quanto à precisão do alinhamento dos troços de fibra que se pretende ligar.

A fragilidade e o pequeno alongamento axial permitido pelas fibras óticas influenciam a estrutura dos cabos. Ao contrário dos cabos tradicionais onde os condutores ajudam a suportar a carga, deve ser evitado qualquer tipo de tensão axial sobre fibras óticas. Para atingir este resultado recorre-se à introdução na construção dos cabos de elementos de resistência que absorvam as tensões axiais, tais como: fio de aço, fibras de vidro, Kevlar, fibras de carvão e fios de plástico.

Num cabo de fibras óticas podem também ser incorporados condutores de cobre ou de alumínio para telealimentação dos repetidores. Cabos para fins imunes aos impulsos eletromagnéticos não devem ter elementos metálicos.

Não desenvolvo considerações sobre fibras multimodo dado que não foram por nós utilizadas nos projetos de SITEP.

Emendas em fibras óticas

Os cabos são fornecidos em comprimentos típicos de 1 e 2 km, havendo de realizar emendas permanentes em troços incorporados em ligações que cubram maiores distâncias. As perdas nas juntas têm de ser rigorosamente controladas para possibilitar a redução de perdas e facilitar a otimização entre repetidores ou equipamentos terminais. Também são introduzidas perdas em juntas não permanentes, os ligadores óticos existentes nos contactos entre fibra ótica e respetivo terminal ou repetidor.

Existem dois processos básicos de realização de juntas: a fusão e os ligadores com adaptação do índice de refração. A realização de juntas pelo processo de fusão é o mais vulgarmente praticado consistindo na aplicação de calor localizado na zona da junção entre duas fibras previamente cortadas e alinhadas, provocando a fusão por intermédio de raios laser.

A experiência com que ficamos com estes materiais leva-nos a concluir que o modo de preparar a fibra para a fusão é um dos parâmetros que mais influenciam a atenuação provocada pela soldadura.

Os terminais das fibras devem ser cortados com todo o rigor, após removido o revestimento secundário (bainha). As fibras devem ser convenientemente limpas antes de as colocar na máquina de fusão. Nesta, o alinhamento tem de ser perfeito e pode ser feito manualmente por intermédio de um microscópio ou automaticamente.



Fibra Ótica emendada por fusão



Primeiramente é feita a pré-fusão com as fibras ligeiramente afastadas, utilizando uma descarga com menos energia para arredondar as superfícies terminais das fibras e evitar a formação de bolhas na soldadura. Finalmente é realizada a fusão definitiva, sendo medida a atenuação resultante da emenda. Se esta se encontra dentro dos parâmetros exigidos é-lhe aplicada uma manga de proteção na zona da fusão com o objetivo de aumentar a resistência mecânica. Se a emenda produz uma atenuação superior ao normal, a fibra é partida e são repetidos todos os passos para nova emenda.

O valor típico de perdas em juntas de fusão em fibras monomodo é de 0,2dB.

Outro processo de junção de fibras que também se aplica na preparação das terminações para ligar a equipamentos terminais é o uso de ligadores, conforme figura. Referimos estes ligadores porque também os aplicámos nos nossos projetos. Existem ligadores para uma ou para várias fibras, sendo estes últimos normalmente utilizados para aplicações militares.

Os ligadores óticos dividem-se em três partes:

- Terminações da Fibra (para proteger os seus terminais);
- Guia de alinhamento (que protegem a fibra para o alinhamento ótico);
- Revestimento do ligador que protege os contactos óticos do meio exterior, mantém as guias alinhadas e as fibras no lugar.

Como terminações das fibras são usadas cápsulas metálicas conhecidas por ponteiras (*ferrules* em inglês). O ar existente entre os terminais de duas fibras no interior dos ligadores pode ser substituído por geleia com um índice de refração próximo da das fibras, o que diminui as perdas por reflexão. Em estações de redes locais é possível avaliar a qualidade da junção no ligador pela observação da intensidade de luz perdida por radiação na junção.



ST

All fiber-optic connectors use ferrules to hold the ends of the fiber and keep them properly aligned.



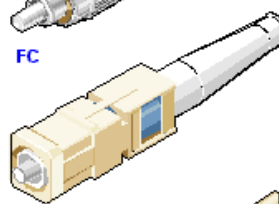
SMA Type 906

The ST connector uses a half-twist bayonet type of lock, while SMA and FC use threaded connections.



FC

The SC uses a push-pull connector similar to common audio and video plugs and sockets.



SC

The MIC is the standard FDDI connector.



MIC

The Fiber Jack connector attaches two fibers in a snap lock connector similar in size and ease of use as an RJ-45 connector.



Fiber Jack

MT-RJ is a popular connector for two fibers in a very small form factor.



MT-RJ

Um operador experiente consegue juntas de fibra com ligadores cujo valor de perdas ronda os 0,3dB.

Lançamento de cabo de fibra ótica

As equipas de montadores de cabos do STM estiveram envolvidas no lançamento de cabos óticos entre o Regimento de Transmissões (STM) e o EME (1986). Há neste projeto um troço de cerca de 1000 metros de cabo, que foi o primeiro fabricado em Portugal, pela fábrica CEL CAT e está incorporado no primeiro projeto do Exército que incluiu fibra ótica (PTAP - Projeto Tipo de Área Piloto).



PTAP - Abertura de vala. Rua da Verónica

A ligação por fibra ótica entre o EME e o STM marcou o início do emprego de fibras óticas nas comunicações do Exército e consolidou a ideia da necessidade da implantação desta tecnologia em ligações locais para o futuro nomeadamente na Área Nodal de Lisboa. A fibra ótica é também indiscutivelmente melhor do que os outros meios para ligar centrais satélites em redes locais e entre centrais telefónicas e estações terminais de feixes hertzianos, tirando partido da transmissão digital, da largura de banda e da imunidade às radiações eletromagnéticas (interferências).

O cabo lançado entre o STM e o EME é um cabo de seis fibras com tensor central em aço e revestimento exterior de polietileno. Sai do RT pela Rua Nossa Senhora da Glória, que percorre até ao fim, onde flete para a Feira da Ladra pela Rua da Verónica, passando depois pela DAT, de onde desce para o EME. Tem emendas junto da Messe Militar de S.ta Clara.

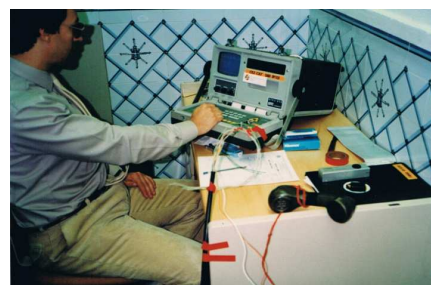
Os cabos são lançados por troços. A escolha de cada troço obedece à análise criteriosa de fatores como:

- Comprimento do traçado completo;
- Curvaturas e inclinação das tubagens;
- Localização das bobines para lançamento no terreno;



PTAP – Emenda por fusão da fibra ótica

- Tipo físico do cabo (diâmetro, resistência mecânica e raio de curvatura aceite);
- Comprimento da cada bobine;
- Tipo de destorcedores a utilizar.



PTAP – Medida de atenuação da fibra ótica

Planeamento

Com alguma antecedência em relação às necessidades de emprego o STM mandou uma equipe chefiada pelo Cap Porfírio tirar um curso de cabos óticos. Ocorreu que, já depois do curso e antes da instalação do cabo ótico entre o STM e o EME, o STM foi desafiado a lançar um cabo de fibra ótica para a NATO, entre a EMEL e o CINCIBERLANT, iniciando a equipe acima a sua atividade de campo com esta obra. Trata-se de um cabo de 6 fibras, tensor central em Kevlar, sem qualquer elemento metálico e com uma extensão de 4200 metros, fornecido em troços de 1000m, 1350m e 1850m.

Deste modo e quase por acaso a equipe de STM ganhou experiência prévia numa obra que antecedeu, com fibra importada, a do lançamento do PTAP.



História

Viaturas Automóveis de Projetores

Ao Serviço do Regimento de Telegrafistas, de 1927 a 1940



Luís Costa

“A utilização dos Auto Projetores não se limitou apenas à utilização na instrução da especialidade de telegrafia ótica. Foram diversas as situações em que foram utilizados em cooperação com outras unidades do Exército (...)

Em 1 de Setembro de 1926 foi determinado pela Direção da Arma de Engenharia a organização do Regimento de Telegrafistas³². A sua organização foi definida em 15 de Outubro de 1926, e o Regimento ficou organizado em Comando e Estado Maior, cinco Companhias de Telegrafistas por Fios, duas Companhias de Telegrafistas sem Fios e uma Companhia de Parque³³. Meses depois, foi atribuída uma nova organização definitiva para o Regimento, decretada através do Decreto nº 13.851 publicado em Ordem do Exército, o qual passou a ter nova organização que compreendia: 1º Grupo com duas Companhias de Telegrafistas por Fios e uma Secção de Parque; 2º Grupo com três Companhias de Telegrafistas sem Fios e uma Companhia de Parque e Viaturas; 3º Grupo com uma Companhia de Telegrafistas sem Fios, uma Companhia de Eletromecânicos e uma Companhia de Projetores³⁴. Estava criada a unidade de Projetores do Regimento de Telegrafistas.

A história dos Auto Projetores nos Telegrafistas

Em Junho de 1927 o Regimento de Telegrafistas recebeu as suas primeiras quatro viaturas “Auto Projector”³⁵, destinados à 9ª Companhia do Regimento, a Companhia de Projetores, entretanto formada. Estes “Auto Projector”, que tinham a designação completa de “Auto Projector B.B.Buick”, foram adquiridos em França no ano de 1917 com destino a unidades que guarneciam o Campo Entrincheirado de Lisboa. O Regimento de Telegrafistas recebeu os “Auto Projector B.B.Buick” números 1, 2, 3 e 4³⁶.

A principal finalidade na utilização dos Auto Projetores da Companhia de Projetores do Regimento de Telegrafistas era destinada à realização de sinalização e de telegrafia ótica, mas podiam também serem utilizados para outras finalidades secundárias, consoante as situações em que a Companhia de Projetores fosse utilizada, tais como o reconhecimento de movimentos realizados por forças inimigas e a iluminação de terrenos em movimentações de unidades, entre outras atribuições que competiam a outros Auto Projetores da Arma de Artilharia, tais como a localização e seguimento de aviões inimigos ou a localização de alvos a serem batidos por fogos de Artilharia.

32 Publicado na Ordem Regimental nº 1 de 1 de Setembro de 1926, do Regimento de Telegrafistas.

33 Publicado na Ordem Regimental nº 45 de 15 de Outubro de 1926, do Regimento de Telegrafistas.

34 Publicado na Ordem do Exército nº 7, 1ª série, de Junho de 1927.

35 Designação original tal como foram aumentadas à carga as primeiras viaturas de projetores do Regimento de Telegrafistas. Foram aumentadas através da Ordem Regimental nº 177 de 26 de Junho de 1927, do Regimento de Telegrafistas.

36 Ordem Regimental nº 177 de 26 de Junho de 1927, do Regimento de Telegrafistas.



Estes Auto Projetores eram constituídos pela viatura automóvel de marca *Buick*, pelo projetor da marca *Barbier, Bénard & Turenne* e por todo o equipamento elétrico para utilização do projetor, que funcionavam por meio de um dínamo instalado na viatura e que gerava energia para o projetor. Estes Auto Projetores foram encomendados em 1917 pelo Governo Português á casa comercial *Barbier, Bénard & Turenne* de Paris e os primeiros chegaram a Lisboa em 1918³⁷.

Em Novembro de 1927 a Companhia de Projetores recebeu mais equipamento para o trabalho com os Auto Projetores. Foram recebidos fatos de ganga destinados ao pessoal que trabalhava com os mesmos³⁸.

A utilização dos Auto Projetores da Companhia de Projetores não se limitou apenas à utilização na instrução da especialidade de telegrafia ótica. Foram diversas as situações em que foram utilizados em cooperação com outras unidades do Exército, tais como a que ocorreu no início de Janeiro de 1931, conforme a atribuição do serviço determinada pelo Comandante do Regimento: “(...) Que marcham amanhã para o Destacamento Mixto de Almada, afim de ali acompanharem um Auto Projetor que vai ficar em serviço no mesmo Destacamento, o 2º sargento nº 137/E-C.P., Joaquim Modesto Júnior e 2º cabo nº 759/E-C.P., Augusto Cunha e soldados nº 187/30-C.P., Manuel de Sousa e 889/30-C.P., José Sebastião.”³⁹.

A partir do início dos anos trinta, a designação dos quatro Auto Projetores *Buick* do Regimento passou a ser referida com a designação abreviada de “P.C.1”, “P.C.2”, “P.C.3” e “P.C.4” que se traduzia como

“Projetor de Campanha” seguido do número da viatura⁴⁰.

Em Dezembro de 1933 a Direção da Arma de Engenharia determinou que os Auto Projetores passavam a ser designados pelo número do motor, mesmo que não possuíssem chapa de matrícula⁴¹. Logo em 28 de Dezembro de 1933 o Regimento recebeu outra viatura “Auto Projetor *B.B.Buick*” com o nº 9 e entregou a nº 3, que foi abatida à carga da unidade⁴². Toda a ferramenta e equipamentos da viatura nº 3 foram transferidos para a viatura nº 9. No início de Janeiro de 1934 o Regimento publicou em Ordem Regimental a relação dos seus Auto Projetores e dos respetivos números dos motores:

“Artº 8º - MATERIAL DE PROJETORES: Que para efeitos de registo se publique a relação dos números dos Auto Projetores pertencentes ao Regimento e daqueles que não pertencendo à unidade aqui se encontram destacados:

Auto Projetores da carga do R.T.

P.C.1 (motor nº) 161.052

P.C.2 (motor nº) 161.054

P.C.4 (motor nº) 213.071

P.C.9 (motor nº) 160.992 (...)

Auto Projetores do D.M.E. da Pontinha

Charron (motor nº) 22.863

Buick (motor nº) 160.994 (...)”⁴³.

Além dos Auto Projetores *Buick* do Regimento, esta relação refere também a existência de um Auto

37 Nota confidencial nº 114 de 3 de Agosto de 1918 da 2ª Direção Geral da Secretaria da Guerra, A.H.M. 1ª Div. 35ª Sec. Cx. 123.

38 Aumentados à carga do Regimento através da Ordem Regimental nº 330 de 26 de Novembro de 1927, do Regimento de Telegrafistas.

39 Determinação de serviço publicada na Ordem Regimental nº 8 de 8 de Janeiro de 1931, do Regimento de Telegrafistas.

40 Designações abreviadas que aparecem publicadas na Ordem Regimental nº 295 de 22 de Outubro de 1931, do Regimento de Telegrafistas.

41 Determinado pela nota nº 3.489/8-P da 2ª Repartição da Direção da Arma de Engenharia de 19 de Dezembro de 1933, publicado na Ordem Regimental nº 356 de 22 de Dezembro de 1933, do Regimento de Telegrafistas.

42 Abate do Auto Projetor nº 3 e aumento do Auto Projetor nº 9 através da Ordem Regimental nº 363 de 29 de Dezembro de 1933, do Regimento de Telegrafistas.

43 Publicado na Ordem Regimental nº 4 de 4 de Janeiro de 1934, do Regimento de Telegrafistas.



Projektor *Charron* e de um Auto Projektor *Buick* pertencentes ao Depósito de Material de Engenharia situado na Pontinha e que estavam em diligência no Regimento de Telegrafistas.



Um “Auto Projektor *Charron*” em exercícios de utilização do Projektor *Barbier, Bénard & Turenne* (Coleção Luís Costa).

Em 9 de Fevereiro de 1934 o Regimento recebeu mais quatro Auto Projetores para a Companhia de Projetores, os quais foram aumentados à carga do Regimento com os respetivos números de matrícula, não se utilizando a discriminação dos números dos motores dos mesmos. Estes Auto Projetores, então recebidos das Oficinas Gerais de Material de Engenharia, foram os “Auto Projektor *Charron*” nº M.G. 17, M.G. 18, M.G. 19 e M.G. 20⁴⁴. Com estes Auto Projetores estava então a ser utilizado outro sistema de matrículas, no qual se utilizava em vez do número de “Projektor de Campanha” seguido do número da viatura, uma matrícula com as letras M.G. do Ministério da Guerra seguido do respetivo número da viatura.

Estas viaturas “Auto Projektor *Charron*” foram também recebidas da casa comercial *Barbier, Bénard & Turenne* de Paris, e tal como os *Buick* eram constituídos pela viatura automóvel de marca *Charron*, pelo projektor da marca *Barbier, Bénard & Turenne* e por todo o equipamento elétrico para utilização do projektor.

44 Publicado na Ordem Regimental nº 46 de 15 de Fevereiro de 1934, do Regimento de Telegrafistas.

Em 28 de Fevereiro de 1934 foi abatido o “Auto Projektor *Buick*” com o número de motor 160.992 e já designado com a matrícula M.G. 9, em vez do registo P.C. 9, que foi substituído pela matrícula do Ministério da Guerra⁴⁵. Na mesma data deixou de estar em diligência no Regimento o “Auto Projektor *Charron*” M.G. 22 com o número de motor 22.863, pertencente ao Depósito de Material de Engenharia⁴⁶.

Em 21 de Novembro de 1934 o Regimento de Telegrafistas recebeu outro “Auto Projektor *Charron*” que foi atribuído ao 1º Grupo do Regimento que estava destacado na cidade do Porto. Foi recebido o “Auto Projektor *Charron*” com a matrícula M.G. 31⁴⁷.

Para colmatar a falta do “Auto Projektor *Buick*” M.G. 9 na Companhia de Projetores, abatido em Fevereiro de 1934, foi recebido em 28 de Fevereiro de 1935 outro “Auto Projektor *Buick*” com a matrícula M.G. 8⁴⁸. Com a chegada deste Auto Projektor a Companhia de Projetores ficou equipada com quatro “Auto Projektor *Buick*” e quatro “Auto Projektor *Charron*”. Em Novembro deste ano houve nova alteração na existência dos Auto Projetores do Regimento, sendo entregues os “Auto Projektor *Charron*” matrículas M.G. 17 e M.G. 18 e foram recebidos os “Auto Projektor *Charron*” matrículas M.G. 25 e M.G. 26⁴⁹. Estes movimentos de entradas e saídas destas viaturas deveram-se a grandes trabalhos de reparações a que estas viaturas necessitavam e que obrigavam a serem substituídas umas por outras nas unidades operacionais. Em Novembro de 1936 o “Auto Projektor *Charron*” com a matrícula M.G. 18, que já tinha pertencido ao Regimento, foi de novo entregue ao Regimento de

45 Abate efetuado através da Ordem Regimental nº 61 de 2 de Março de 1934 e complementada pela Ordem Regimental nº 313 de 9 de Novembro de 1934, do Regimento de Telegrafistas.

46 Determinado na Ordem Regimental nº 61 de 2 de Março de 1934 do Regimento de Telegrafistas.

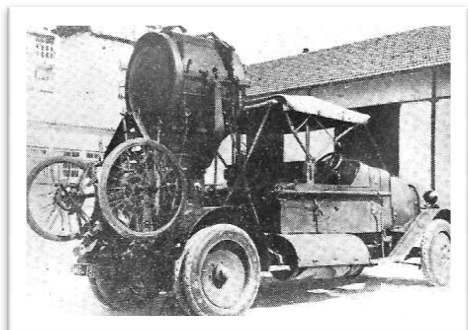
47 Aumentado á carga através da Ordem Regimental nº 328 de 24 de Novembro de 1934 do Regimento de Telegrafistas.

48 Aumentado á carga através da Ordem Regimental nº 82 de 23 de Março de 1935 do Regimento de Telegrafistas.

49 Movimento efetuado através da Ordem Regimental nº 82 de 23 de Março de 1935 do Regimento de Telegrafistas.



Telegrafistas⁵⁰ para substituir o “Auto Projetor Charron” M.G. 19, o qual foi enviado para as Oficinas Gerais de Material de Engenharia e foi abatido à carga do Regimento⁵¹.



O “Auto Projetor Charron” M.G. 18 visto detrás, onde se pode ver o Projetor montado no chassis. (Coleção Luís Costa).

Os últimos tempos ao serviço dos Telegrafistas

A situação técnica dos Auto Projetores do Regimento foi-se agravando com o passar do tempo e as avarias sucederam-se de tal forma que alguns foram sendo abatidos e substituídos consoante as disponibilidades de outras viaturas para tomarem o seu lugar na Companhia de Projetores. Assim, em Dezembro de 1936 foi abatido o “Auto Projetor Buick” M.G. 2, logo seguido em Fevereiro de 1937 pelo “Auto Projetor Buick” M.G. 8⁵². Este último encontrava-se em serviço no Forte do Alto do Duque, onde foi substituído pelo “Auto Projetor Charron” M.G. 20⁵³. Em 13 de Fevereiro de 1937 foi recebido de novo o “Auto Projetor Charron” M.G. 19 que tinha sido enviado para grande reparação nas Oficinas Gerais de Material de Engenharia, o qual foi de novo aumentado à carga do Regimento e entregue à Companhia de Projetores⁵⁴. O mesmo

aconteceu com o “Auto Projetor Charron” M.G. 31 que estava atribuído ao 1º Grupo do Regimento destacado na cidade do Porto, o qual foi abatido e substituído pelo “Auto Projetor Charron” M.G. 17, que já tinha pertencido ao Regimento⁵⁵. A 24 de Julho de 1937 foi a vez do “Auto Projetor Charron” M.G. 20, em serviço no Forte do Alto do Duque, que teve de ser substituído pelo “Auto Projetor Buick” M.G. 4, por causa de avarias no primeiro⁵⁶.

Em meados de Fevereiro de 1940 foi publicado em Ordem do Exército o Decreto nº 29.957 o qual determinou a extinção do Regimento de Telegrafistas e a formação do Batalhão de Telegrafistas, bem como a transferência do 1º Grupo do Regimento de Telegrafistas que estava destacado no Porto, para o Regimento de Engenharia nº 1 onde passou a constituir o Batalhão de Transmissões deste Regimento⁵⁷. Na organização do Batalhão de Telegrafistas não foi prevista a Companhia de Projetores que então foi extinta com a extinção do Regimento de Telegrafistas⁵⁸. Todo o material do extinto Regimento de Telegrafistas foi transferido para o Batalhão de Telegrafistas, mas aos poucos o material que foi considerado desnecessário ao funcionamento do Batalhão foi abatido. Tal aconteceu com os Auto Projetores que já não tinham utilização no Batalhão de Telegrafistas. A 16 de Julho de 1940, todos os “Auto Projetor Buick” e os “Auto Projetor Charron”, bem como todo o material sobresselente destas viaturas foram abatidos à carga do Batalhão de Telegrafistas⁵⁹. Terminavam mais de doze anos de utilização destas viaturas especiais ao serviço dos Telegrafistas e da Arma de Engenharia.

50 Aumentado à carga através da Ordem Regimental nº 309 de 4 de Novembro de 1936 do Regimento de Telegrafistas.

51 Abatido à carga através da Ordem Regimental nº 318 de 10 de Novembro de 1936 do Regimento de Telegrafistas.

52 Abatidos à carga através da Ordem Regimental nº 350 de 15 de Dezembro de 1936 e da Ordem Regimental nº 51 de 20 de Fevereiro de 1937 do Regimento de Telegrafistas.

53 Substituição no serviço de projectores no Forte do Alto do Duque, referido na Ordem Regimental nº 27 de 27 de Janeiro de 1937 do Regimento de Telegrafistas.

54 Aumentado à carga através da Ordem Regimental nº 56 de 25 de Fevereiro de 1937 do Regimento de Telegrafistas.

55 Movimento de abate e aumento à carga efectuado através da Ordem Regimental nº 148 de 28 de Maio de 1937 do Regimento de Telegrafistas.

56 Substituição determinada pela Ordem Regimental nº 208 de 27 de Julho de 1937 do Regimento de Telegrafistas.

57 Publicado na Ordem Regimental nº 60 de 29 de Fevereiro de 1940 do Regimento de Telegrafistas.

58 Ordem Regimental nº 56 60 de 29 de Fevereiro de 1940 do Regimento de Telegrafistas. Esta é a última Ordem Regimental do Regimento de Telegrafistas.

59 Abatidos à carga através da Ordem de Serviço nº 145 de 23 de Julho de 1940 do Batalhão de Telegrafistas.



Ambiente

A contribuição das U/E/O do Exército para o Programa ECO.AP



Carlos Sequeira

Maj Tm (Eng)

Com a Resolução do Conselho de Ministros (RCM) Nº2/2011 de 12 de janeiro é lançado o Programa de Eficiência Energética na Administração Pública (ECO.AP), nomeadamente nos seus serviços, edifícios e equipamentos, tendo como objetivo principal a obtenção, até 2020, de um nível de eficiência energética na ordem dos 20% em relação aos valores atuais, ou seja, reduzir em 20% as emissões de carbono (CO₂). A RCM Nº20/2013 de 10 abril de 2013, e no quadro das metas europeias «20-20-20», estabelece para Portugal, para o mesmo horizonte 2020, um objetivo geral de redução de energia primária de 25% e um objetivo específico para a AP de redução de 30%.



eco·ap

Programa de Eficiência Energética
na Administração Pública

“... o Programa de Eficiência Energética na Administração Pública (ECO.AP), tem como objetivo principal a redução, até 2020, de 20% das emissões de carbono (CO₂)...”

Neste contexto, foram traçadas algumas medidas, sendo de destacar, no caso concreto do Exército, a nomeação dos Gestores Locais de Energia e Carbono (GLEC) em todas as Unidades, Estabelecimentos e Órgãos do Exército (U/E/O), concorrendo assim para uma única rede de GLEC na AP, bem como a criação do Barómetro de eficiência da AP, com a finalidade de comparar e divulgar ao público o desempenho energético dos serviços da AP.

Com a implementação deste Barómetro ECO.AP pretende-se, também, obter uma visão global sobre o grau de eficiência energética na utilização dos edifícios e frotas das entidades da AP, apontando o Estado como referência na gestão dos consumos de energia e promotor de boas práticas de eficiência energética e baixo carbono, facilitando aos ministérios a identificação das entidades que representam 20% do seu consumo total, bem como a identificação de metas para planos de ação de Eficiência Energética e de Baixo Carbono (EEBC). Estes planos têm como objetivo promover uma economia de baixo carbono na AP, contribuindo para a redução de emissões de Gases com Efeito de Estufa (GEE) nas áreas de competência dos diferentes ministérios, baixando custos e promovendo a eficiência na gestão de recursos.



Barómetro ECO.AP

(Fonte: <http://www.adene.pt/pt-pt/NavegacaoDeTopo/EnergiaNoEstado/EcoAP/Documents/120124BarometroEE.pdf>)

Significa isto que, ao nível do Ministério da Defesa e para o caso concreto do Exército, cada GLEC nomeado, para a respetiva U/E/O, terá de fazer um levantamento exaustivo de todos os seus edifícios (analisando as áreas, os equipamentos instalados e suas características, os consumos elétricos, etc.), de toda a frota existente e consumos de combustível, de todo o pessoal militar/civil existente (apresentando de forma qualitativa os seus comportamentos), dos consumos de água e do papel consumido pela respetiva U/E/O. Com estes dados introduzidos no Barómetro é então feito o cálculo do índice ECO.AP de acordo com a figura apresentada a seguir.

Segue-se uma análise em pormenor de algumas medidas que podem ser tomadas pelo GLEC e que contribuem de forma significativa para a eficiência energética da sua U/E/O, e consequentemente para o Programa ECO.AP:

1. Propor a substituição de lâmpadas de baixa eficiência energética por lâmpadas mais eficientes, não só no interior dos edifícios como em toda a

envolvente externa dentro do perímetro das U/E/O (candeeiros de rua). Interessa referir que existem no mercado algumas tecnologias emergentes como as *Light-Emitting Diode* (LED) ou o halógeno eficiente, que pelo seu baixo consumo se prevê que comecem a substituir as lâmpadas destinadas à sinalização e a outras utilizações mais comuns das lâmpadas incandescentes de baixa eficiência. Nesta medida, apesar de as lâmpadas serem consideravelmente mais caras, consegue-se um *payback* que a curto/médio prazo, de acordo com a taxa de utilização, compensará o investimento.

2. Analisar o consumo de energia elétrica pelas faturas, solicitando apoio a uma empresa de Serviços Energéticos (ESE) com enquadramento dado pelo DL 29/2011 de 28 de fevereiro, que estabelece acordos contratuais celebrados entre a Entidade Pública e a ESE, com a finalidade de apresentar um estudo que torne a U/E/O o mais eficiente possível dentro das metas acordadas, em que os investimentos são pagos consoante as economias de energia resultantes.



Cálculo do Índice ECO.AP

Área	Indicador	Ponderação	Pontuação
Energia edifícios	kWh/m² útil	35%	Valor da entidade em cada indicador/valor mínimo nesse indicador x 100
Energia frota	kWh/100 km	25%	
Carbono	CO ₂ e/colaborador	20%	
Comportamentos	Perguntas qualitativas	10%	
Água	m³/colaborador	5%	
Papel	resmas/colaborador	5%	

A soma das pontuações ponderadas obtidas pelas entidades nas 6 áreas avaliadas determina a sua avaliação final pelo Índice ECO.AP

Cálculo do índice ECO.AP

(Fonte: <http://www.slideshare.net/construcaosustentavel/dinis-rodrigues-adene-13431737>)

3. Analisar a fatura do gás e verificar se no mercado existem soluções mais eficientes. Como exemplo veja-se o seguinte caso: se a U/E/O for fornecida por botijas/depósito de gás butano/propano deve ser equacionada a possibilidade de instalação de uma rede de fornecimento de gás natural, pois o metro cúbico é substancialmente mais barato e este gás produz uma combustão mais limpa, que emite uma menor quantidade de dióxido de carbono para a atmosfera, quando comparado com outras fontes de energia fósseis.

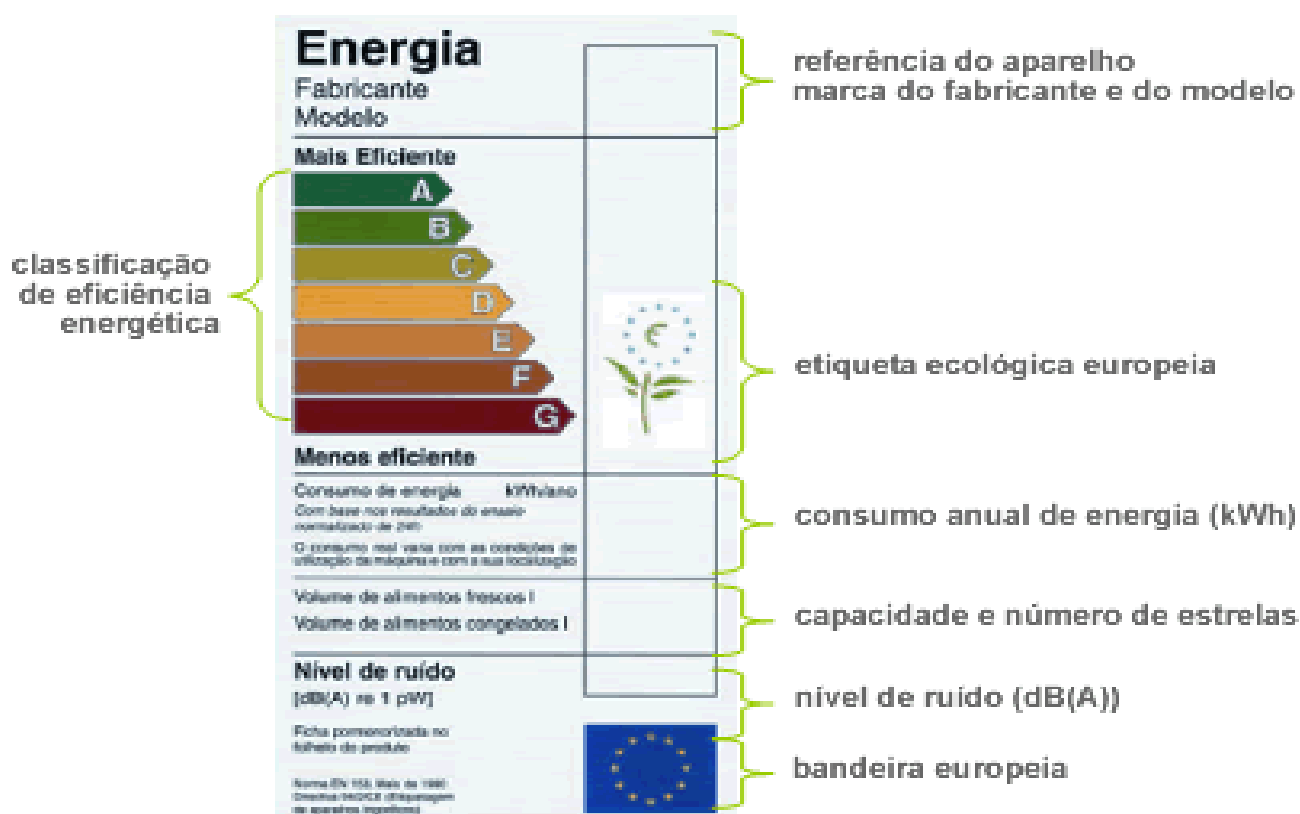
4. Considerando que o parque automóvel das U/E/O está, de um modo geral, obsoleto. Nomeadamente as viaturas administrativas, com consumos de combustível superiores aos consumos das viaturas mais recentes e com emissões de gases poluentes superiores. Tendo isto em consideração o GLEC poderá tomar algumas iniciativas como: propor o abate de viaturas em que a sua manutenção deixou de ser viável, cumprir rigorosamente os planos de manutenção das viaturas e aconselhar a coordenação de deslocamentos de forma a transportar o máximo de pessoas com o mínimo de viaturas, optando sempre pelas de baixo consumo. Para tal, deverá

existir um registo de consumos de combustível e de distâncias percorridas por viatura.

5. Propor, dentro da capacidade financeira da U/E/O ou da existência no canal Logístico, a substituição de todos os equipamentos obsoletos e de baixa eficiência como caldeiras, fornos, geradores, máquinas de lavar loiça/roupa, equipamentos de frio, etc., por equipamentos de maior eficiência de acordo com a respetiva etiqueta de “eficiência energética”, obrigatória por lei, e apresentada na página seguinte.

6. Reduzir a fatura da água através da instalação de filtros redutores de caudal em todas as torneiras e chuveiros, ou só nestes últimos, que representam o equipamento com maior consumo de água. Deverá existir, na U/E/O, um registo diário de consumos de água, de forma a despistar qualquer desperdício provocado por anomalias na rede de distribuição ou torneiras/chuveiros mal fechados.

7. Envolver todas as pessoas da U/E/O num programa de eficiência energética, divulgando todo o tipo de informação nesta área (ex: através do portal da U/E/O ou afixando documentos em locais próprios). Esta medida é de extrema importância, pois a atitude das pessoas é das mais valiosas fontes de poupança.



Etiqueta de eficiência energética

(Fonte: <http://joanadavid.webnode.pt/etiqueta%20de%20efici%C3%Aancia%20energetica/>)

Conclusões

Analisando estas medidas, e em forma de conclusão, pode-se afirmar que sem efetuar uma alteração profunda ao nível da estrutura dos edifícios das U/E/O, principalmente dos quartéis do Exército inseridos no programa de construção e remodelação da antiga Comissão Administrativa das Novas Instalações para as Forças Armadas (CANIFA), consegue-se uma poupança energética significativa. Isto é, seria bastante oneroso, numa altura de contenção financeira, tornar estas estruturas o mais eficiente possível substituindo envidraçados, caixilharias, portas, sistemas de aquecimento/arrefecimento de edifícios, etc., com a agravante de as paredes construídas em meados do século XX não possuírem o isolamento térmico que as estruturas mais modernas exigem.

Todo o tipo de medidas que puderem vir a ser tomadas em prol da eficiência energética traduzem, na prática, uma redução do consumo das fontes

secundárias de energia (gasóleo, gasolina e eletricidade), ou seja, tornando a frota mais eficiente é necessário menos consumo destes dois primeiros, e se se conseguir reduzir a fatura de eletricidade, reduz-se o consumo da última. Com isto, e porque as fontes secundárias de energia são obtidas a partir de fontes primárias, reduz-se, consequentemente, a necessidade de consumo destas últimas (carvão, petróleo e gás natural), e diminui-se, de forma direta, as emissões de CO₂ e dos GEE, contribuindo assim para o objetivo principal deste programa ECO.AP.

Bibliografia

- www.operacional.pt/os-quarteis-canifa/
- <http://ambiente.maiadigital.pt/ambiente/energia/mais-informacao-1/sobre-as-questoes-energeticas/>
- <http://ambiente.kazulo.pt/5000/combustiveis-fosseis-e-poluicao.htm>
- www.adene.pt/
- <http://dre.pt/pdf1sdip/2011/01/00800/0027000271.pdf>
- <http://dre.pt/pdf1sdip/2013/04/07000/0202202091.pdf>



Resumo de Atividades

SETEMBRO

DIA DO REGIMENTO DE TRANSMISSÕES

Foi com simplicidade mas muita dignidade, que no dia 17 de setembro de 2012 se comemorou o 35º aniversário do Regimento de Transmissões, cerimónia que foi presidida pelo Comandante das Forças Terrestres, o Exmo. TGen Carlos António Corbal Hernandez Jerónimo e que contou com a presença de ilustres convidados militares e civis.



A cerimónia militar foi complementada com uma atuação da Banda do Exército, ao que se seguiu a cerimónia de inauguração da sala do Centro de Sistemas Operacionais do Exército, atividades com as quais se pretendeu assinalar simbolicamente o dia festivo do Regimento de Transmissões.



As comemorações do dia do Regimento terminaram com o tradicional almoço, durante o qual diferentes gerações de militares deste Regimento bem como os restantes convidados militares e civis puderam usufruir de um franco convívio.

TOMADA DE POSSE DO COMANDANTE DO RT

Em 19 de setembro de 2012, teve lugar a cerimónia de tomada de posse do Exmo. Coronel Transmissões Engenheiro Antonino Melchior Pereira de Melo, como Comandante do Regimento de Transmissões.

Após a cerimónia militar decorreu no salão nobre a apresentação de cumprimentos dos militares e civis que prestam serviço no RT. Seguiu-se um bríngue e visita à unidade.



DESPEDIDA DE MILITARES

Realizou-se no dia 26 de setembro de 2012 uma cerimónia de despedida dos militares que por motivos de serviço mudaram a sua unidade de colocação. Esta cerimónia decorreu na messe de Sargentos do RT, tendo contado com a presença de todos os Oficiais, Sargentos e Civis.



CERIMÓNIA DE PROMOÇÃO

Decorreu no dia 27 de setembro de 2012, no salão nobre do Regimento de Transmissões, a cerimónia de promoção dos AspOf RC Neto, AspOf RC Duarte, AspOf RC Fonseca, AspOf RC Silva e 2Furr RC Lopes. A cerimónia foi precedida do tradicional porto de honra.



OUTUBRO

DÁDIVA DE SANGUE

O Regimento de Transmissões recebeu no dia 03 de Outubro de 2012, uma equipa do Instituto Português de Sangue e da Transplantação, com um efetivo de quatro elementos, dos quais, um médico, uma enfermeira, uma técnica e uma administrativa, com o objetivo de realizar recolhas de sangue a fim de poder contribuir para um aumento de concentrados eritrocitários, plaquetas e plasma do Banco de Sangue, bem como a recolha de sangue para o banco de dados de doadores de medula óssea. A forte adesão dos militares a esta causa faz realçar o espírito de corpo e entreajuda que a instituição mantém há

séculos. Foram realizadas vinte e sete colheitas de sangue, dos quais cinco são doadores pela primeira vez e três deles inclusive, propuseram-se para a tipagem de doadores de medula óssea. O Regimento de Transmissões com esta iniciativa veio fortalecer mais uma vez a divisa que o IPST instiga, “Dar sangue é dar vida.”



CERIMÓNIA DE PROMOÇÃO

Decorreu no dia 08 de outubro de 2012, no salão nobre do Regimento de Transmissões, a cerimónia de promoção do 2Furr RC Mota. A cerimónia foi precedida do tradicional porto de honra.



CERIMÓNIA DE PROMOÇÃO

Decorreu no dia 10 de outubro de 2012, no salão nobre do Regimento de Transmissões, a cerimónia de promoção do 2Sarg Tm Amaral, 2Sarg Tm Caetano e 2Sarg Tm Reis Araújo. A cerimónia foi precedida do tradicional porto de honra.



APRONTAMENTO DA MPCOY/NRF 2013

Decorreu no Regimento de Transmissões no período de 08 a 12 de Outubro de 2012, um estágio de Transmissões Permanentes e Segurança das Transmissões para o aprontamento da MPCOY/NRF 1º Semestre de 2013, a qual foi frequentada por dois formandos, um 1º Sargento e um 2º Sargento deste Regimento.”



PROGRAMA PARA A PREVENÇÃO E COMBATE À DROGA E AO ALCOOLISMO NO EXÉRCITO

No âmbito do Plano de Atividades para este período do Programa para a Prevenção e Combate à Droga e ao Alcoolismo no Exército, foi realizado um rastreio toxicológico aleatório a diversos Oficiais, Sargentos e Praças do RT.

CERIMÓNIA DE DESPEDIDA DO CHEFE DO CSI

Em 12 de outubro de 2012 decorreu a cerimónia de despedida do TCor Tm (Eng) Vitor Terras Chefe do Centro de Segurança da Informação, por motivo de ter sido nomeado por escolha para 2Cmndt da Escola

Prática de Transmissões. A cerimónia foi precedida de um almoço de convívio.



CERIMÓNIA DE PROMOÇÃO

Decorreu no dia 22 de outubro de 2012, no salão nobre do Regimento de Transmissões, a cerimónia de promoção do Ten Tm (Eng) Dias. A cerimónia foi precedida do tradicional porto de honra.



NOVEMBRO

TIRO DE MANUTENÇÃO

Em 28 de novembro de 2012, realizou-se o Tiro de Manutenção Anual (TMA), relativo ao ano de 2012, de todos os militares do RT. O tiro de Esp. Aut. G3 e Pistola Walther, foi realizado nas Carreiras de Tiro da EPI em Mafra.



VISITA DE ESTUDO DO TIROCÍNIO DO ESTÁGIO TÉCNICO MILITAR – ESPECIALIDADE TOCC DA FAP

Em 29 de novembro de 2012, dois formandos e um formador do Tirocínio do Estágio Técnico Militar da especialidade de TOCC da Força Aérea Portuguesa, efetuaram uma visita de estudo ao Regimento de Transmissões. A visita esteve centrada nas Comunicações e Sistemas de Informação e Segurança da Informação implementadas pelo RT em prol do Exército. Para o efeito, aos visitantes foi proporcionado um briefing sobre o tema e uma visita ao Batalhão de Comunicações e Sistemas de informação e ao Centro de Segurança da Informação.



DEZEMBRO

INSPEÇÃO DE SEGURANÇA AO MATERIAL DE GUERRA

Em 06 de dezembro de 2012 realizou-se uma inspeção de segurança ao material de guerra do RT. Esta inspeção foi chefiada pelo MGen Raul Cunha da Inspeção Geral do Exército.



ALMOÇO DE NATAL

Em 19 de dezembro de 2012 realizou-se um almoço de Natal com a participação de todos os Oficiais, Sargentos, Praças e Civis do RT e também extensível aos militares da DCSI e membros da CHT.



JANEIRO

STAND DO RT NA 40ª EXPOSIÇÃO NACIONAL E PRÉ-OLÍMPICA DE COLUMBOFILIA NAS CALDAS DA RAINHA

O Exército através do Regimento de Transmissões esteve presente na 40ª Exposição Nacional e Pré-Olímpica de Columbofilia, que decorreu no Pavilhão Expoeste, nas Caldas da Rainha, no período de 10 a 13 de janeiro de 2013. O stand expôs uma mostra columbófila com um conjunto de artigos históricos do pombal militar nº1 de Lisboa, no sentido de divulgar a sua história, como um dos meios de comunicação que foram empregues historicamente no Exército em Portugal.



APRONTAMENTO DA FND KFOR

No período de 14 a 18 janeiro de 2013, inclusive, decorreu o estágio de Transmissões Permanentes e Segurança das Transmissões para o aprontamento da FND/KFOR com cinco formandos.



FEVEREIRO

COLHEITA DO CENTRO DE HISTOCOMPATIBILIDADE DO SUL

Em 01 de fevereiro de 2012, uma equipa de enfermeiros do Centro de Histocompatibilidade do Sul (CHSul) agradeceu o Regimento de Transmissões com a sua presença, associada a tão ilustre causa.

O propósito desta intervenção visou catalogar um maior número possível de militares, recolhendo amostras de sangue, para posterior análise nas instalações do CHSul, verificando a histocompatibilidade dos dadores, de modo a associarem-se à base de dados de doadores de medula óssea.



O móbil da sua missão materializou-se de forma excecional, foram recolhidas 51 amostras de sangue

78 | A ALMENARA Nº 5 - 2013

de militares deste RT, dos quais participaram oficiais, sargentos e praças. É de salutar a adesão em massa dos nossos militares a tão nobre causa, e a preocupação constante em ajudar o próximo. Deste modo, o RT agradece ao CHSul e em especial aos enfermeiros Gonçalo e Rita.

APRONTAMENTO DO 6CN/FND/ISAF

No período de 18 a 22 de Fevereiro de 2013, realizou-se neste Regimento de Transmissões um Estágio de Transmissões Permanentes e Segurança das Transmissões a militares que integram o aprontamento da 6CN/FND/ISAF.



PROCISSÃO DO SENHOR DOS PASSOS

Realizou-se no dia 24 de fevereiro de 2013 a tradicional Guarda de Honra do Exército à imagem do Senhor dos Passos – Real Irmandade de Santa Cruz e Passos da Graça. O Regimento de Transmissões esteve presente, neste ato, com uma delegação constituída por um sargento e quatro praças que efetuaram a Guarda de Honra no percurso da Igreja de São Roque para a Igreja da Graça.





ESTÁGIO DO TIROCÍNIO PARA OFICIAIS (TPO) DE TRANSMISSÕES

No período de 25 de fevereiro a 1 de março de 2013 decorreu no Regimento de Transmissões o Estágio do TPO de Tm, constituído por 7 Alferes Alunos. Este estágio permitiu aos futuros Oficiais de Transmissões, contactarem com aquilo que é a atividade diária do RT no âmbito da sustentação do Sistema de Informação e Comunicações Operacional (SIC-Op) e da Segurança da Informação.



MARÇO

PALESTRA DOS ALCOÓLICOS ANÓNIMOS E NARCÓTICOS ANÓNIMOS

No dia 06 de março de 2013 realizou-se neste Regimento de Transmissões uma palestra sobre Alcoolismo e Toxicodependência.



Esta palestra enquadrou-se no âmbito do Programa para a Prevenção e Combate à Droga e ao Alcoolismo no Exército em desenvolvimento no RT e contou com a presença do Dr. Francisco Henriques, Médico Especialista em Comportamentos Aditivos,

acompanhado por Patrícia Oliveira Silva e Mário Dias como Técnicos de Aconselhamento e três utentes da Instituição Rumo Certo que prestaram o seu testemunho.

PALESTRA POR PARTE DA DSP AOS CIDADÃOS PALOP



Em 19 de março de 2013, decorreu no Regimento de Transmissões uma apresentação por parte da Repartição de Apoio Social da DSP aos cidadãos dos Países Africanos de Língua Oficial Portuguesa (PALOP) alojados no RT com vista a efetuar um ponto de situação quanto ao estado do processo de cada um destes ex-militares.

COMEMORAÇÕES DO DIA FESTIVO DA ARMA DE TRANSMISSÕES E DA SUA ESCOLA PRÁTICA

Em 22 de março de 2013, o Regimento de Transmissões participou com uma subunidade de escalão pelotão nas comemorações do dia festivo da Arma de Transmissões e da sua Escola Prática.



CURSO LOGFAS/2013

Em 22 de março de 2013, realizou-se neste Regimento de Transmissões o encerramento do Curso LOGFAS/2013 (Logistics Functional Area Services),



presidida pelo Exmo. Adjunto do Comandante das Forças Terrestres, Major-General Luís Manuel Martins Ribeiro. O Curso decorreu no período de 11 a 22 de março, sob a responsabilidade do Comando das Forças Terrestres, tendo participado três oficiais e cinco sargentos.



ABRIL

VISITA DE TRABALHO DO DIRETOR COORDENADOR DO EME AO RT

No âmbito do processo de reorganização da estrutura do Exército decorreu em 04 de abril de 2013 uma visita de trabalho do EME ao RT. A delegação do EME, da qual faziam parte os chefes das diversas Divisões do EME, era chefiada pelo MGen Rovisco Duarte, Diretor Coordenador do EME.



ESTÁGIO DO 39º CURSO DE QUALIFICAÇÃO DE SARGENTOS DE TRANSMISSÕES

Em 08 de abril de 2013 apresentou-se neste Regimento de Transmissões o 39º Curso de Qualificação de Sargentos de Transmissões, constituídos por 11 Sargentos Alunos para

frequentarem o Estágio de Técnico de Comutação e Redes. O estágio decorreu até 26 de julho de acordo com o Programa Geral e os conteúdos programáticos específicos para a formação de Sargentos de Transmissões, especialidade de Técnico de Comutação e Redes.



RASTREIO TOXICOLÓGICO

Em 11 de abril de 2013 realizou-se uma ação de rastreio toxicológico efetuado por equipas cinotécnicas do RL2.



ENTREGA DE PLACAS/RESERVA/LOUVORES

Decorreu no dia 17 de abril de 2013 a cerimónia de entrega de medalhas, diplomas e placas alusivas de passagem à reserva a militares e civis que prestaram serviço no RT (Cap Lopes, SMor Morais, SAj Esteves e Civil Leonor Costa). Esta cerimónia foi precedida de um almoço.



MAIO

PROCISSÃO DE NOSSA SENHORA DA SAÚDE

Realizou-se no dia 05 de maio de 2013, a tradicional procissão de Nossa Senhora da Saúde, vulgarmente conhecida por Procissão dos Artilheiros. Esta procissão é a mais antiga manifestação de religiosidade popular lisboeta que remonta ao tempo do estabelecimento da soberania portuguesa na cidade.



O Regimento de Transmissões esteve presente, neste ato, com uma delegação constituída por um oficial, um sargento e 6 praças.

PÓLO DE TRANSMISSÕES DO MUSEU DE ELVAS

Decorreu no dia 09 de maio de 2013 o movimento inicial para o Museu de Elvas de parte do espólio da coleção visitável do RT. Este movimento tem como objetivo criar no Museu Militar de Elvas um polo de Transmissões. Este trabalho está a ser coordenado pela CHT.



VISITA DE APOIO TÉCNICO DO LABORATÓRIO DE BROMATOLOGIA

Em 21 de maio de 2013 efetuou-se uma visita de apoio técnico do Laboratório de Bromatologia à Seção de Alimentação do RT. A visita teve por objetivo fazer um estudo de situação, avaliando as condições de funcionamento desta Seção no âmbito da Higiene e Segurança Alimentar (áreas de armazenagem, de preparação, de confeção e de distribuição de géneros alimentícios, copa e refeições).



O Laboratório de Bromatologia constatou, mais uma vez, melhoramentos desde a última visita, e vê como um exemplo positivo a atitude do RT, destacando o empenhamento de todos os colaboradores do setor de alimentação nesta melhoria.

VISITA DE ESTUDO DA ESCOLA SECUNDARIA MARQUÊS DE POMBAL



Em 22 de maio 2013, o RT recebeu a visita da Escola Secundária Marquês de Pombal no âmbito de uma visita de estudo dos alunos do Curso Profissional de Gestão de Equipamentos Informáticos.



A visita teve por objetivo proporcionar o contato destes jovens com conceitos e material alusivo às Comunicações e Sistemas de Informação em uso no Exército. Após um briefing no Auditório da unidade, a cargo do Sr. Major Paulo Branco, seguiu-se a visita ao núcleo museológico das Transmissões onde Sr. Coronel Costa Dias, membro da Comissão da História das Transmissões, efetuou uma síntese da evolução histórica das Transmissões.

PROCISSÃO DE SÃO JORGE E SANTA CRUZ DO CASTELO

Realizou-se no dia 26 de maio de 2013, na paróquia de Santa Cruz do Castelo, a tradicional procissão de São Jorge e Santa Cruz. Esta procissão é a mais antiga manifestação de religiosidade popular lisboeta que remonta ao tempo do estabelecimento da soberania portuguesa na cidade.



O Regimento de Transmissões esteve presente, neste ato, com uma delegação constituída por um oficial,

que procedeu à solene “Entrega das Chaves” e oito praças que transportaram aos ombros o andor do Glorioso Mártir São Jorge “Patrono de Portugal” e “Padroeiro das Forças Armadas”.

CERIMÓNIA DE PASSAGEM À DISPONIBILIDADE



Decorreu no dia 31 de maio de 2013 a cerimónia de entrega de medalha de passagem à reserva de disponibilidade do Ten Estrada, oficial contratado mais antigo a prestar serviço no RT. Esta cerimónia foi precedida de um almoço informal.

JUNHO

APRESENTAÇÃO DO SITE DAS LIÇÕES APRENDIDAS DO EXÉRCITO

No passado dia 7 de junho de 2013 decorreu no Regimento de Transmissões a apresentação final do Site das Lições Aprendidas do Exército, desenvolvido em parceria pela Direção de Doutrina, do Comando de Instrução e Doutrina, e Direção de Comunicações e Sistemas de Informação, do Comando das Forças Terrestres.





A apresentação contou com a presença do Comandante das Forças Terrestres, Sua Ex.^ª Tenente-General Carlos Hernandez Jerónimo do Diretor de Doutrina, Sua Ex.^ª Major-General Martins Ferreira e do Diretor de Comunicações e Sistemas de Informação, Sua Ex.^ª Major-General Xavier Matias.

O site foi desenvolvido pela Seção de Portais do Regimento de Transmissões, em coordenação com a Repartição de Lições Aprendidas da Direção de Doutrina, responsável pela definição dos requisitos funcionais.

Esta apresentação materializou o fim da fase de desenvolvimento do projeto seguindo-se um curto período de validação do sistema, envolvendo a participação de um grupo restrito de utilizadores.



APRONTAMENTO DA FND 2BI/KFOR

No período de 17 a 21 de junho de 2013, realizou-se neste Regimento de Transmissões um Estágio de Transmissões Permanentes e Segurança das Transmissões a militares que integram o aprontamento da FND/KFOR. Foi frequentado por 01 Oficial, 03 Sargentos e 03 Praças do 2BI/KFOR em aprontamento para o Teatro de Operações do KOSOVO. Esta ação de formação teve como objetivo a familiarização com os sistemas de informação e comunicações da FND.



TRADICIONAL SARDINHADA

Em 20 de junho de 2013 realizou-se a tradicional sardinhada do RT. Este almoço convívio contou com a participação de todos os Oficiais, Sargentos, Praças e Civis do RT e foi extensível aos militares de Transmissões da DCSI, DivCSI/EME, DICS/EMGFA e membros da CHT.



JULHO

VISITA DO EXMO. MGEN DIRETOR DA DCSI

Em 04 julho de 2013 o Regimento de Transmissões recebeu a visita do Exmo. Major-General Diretor da Direção de Comunicações e Sistemas de Informação, MGen José Filipe da Silva Arnaut Moreira. À chegada ao Regimento foram-lhe prestadas as Honras militares por uma companhia deste Regimento seguindo-se a apresentação de cumprimentos no Salão Nobre. Sua Exa visitou as instalações seguindo-se um almoço de confraternização. No final o Exmo. Comandante do Regimento, Cor Antonino Melchior Pereira de Melo



efetuiu um briefing acerca da missão e possibilidades da Unidade.



PROMOÇÃO DE MILITARES

Decorreu no dia 11 de julho de 2013, no salão nobre do Regimento de Transmissões, a cerimónia de promoção do 1Sarg Geraldo. A cerimónia foi precedida do tradicional porto de honra.



REGIMENTO DE TRANSMISSÕES AGRACIADO COM A MEDALHA DOURADA DA FEDERAÇÃO PORTUGUESA DE COLUMBOFILIA

No passado dia 13 de julho de 2013, o Regimento de Transmissões foi agraciado com a Medalha Dourada da Federação Portuguesa de Columbofilia (FPC), numa cerimónia na Câmara Municipal de Mira, integrada no campeonato mundial de Columbofilia que se realizou no Columbódromo Gaspar Vila Nova, em Portomar-Mira.

O Regimento de Transmissões esteve presente uma vez mais neste evento com uma “Mostra de Columbofilia” dando mais uma vez conhecimento ao público em geral da história do uso do pombo-correio no Exército Português como ancestral meio de comunicação.



A atribuição da medalha constitui o reconhecimento pelo contributo do Regimento na divulgação e preservação do património histórico associado à Columbofilia. Esse contributo tem atualmente expressão na reativação e manutenção de um pombal militar no Regimento de Transmissões, e pela exposição de material associado à Columbofilia, composta por vários apetrechos utilizados pela columbofilia militar, e que o Exército tem disponibilizado para os principais eventos da FPC.

APRONTAMENTO FND/ISAF 2º SEMESTRE DE 2013

Decorreu no Regimento de Transmissões, no período de 29 de julho a 02 de agosto de 2013, um estágio de Transmissões Permanentes e Segurança das Transmissões para o aprontamento da FND/ISAF 2º semestre de 2013, a qual foi frequentada por seis formandos.





SETEMBRO



CERIMÓNIA DE PROMOÇÃO

Decorreu no dia 03 de setembro de 2013, no salão nobre do Regimento de Transmissões, a cerimónia de promoção do SAj Gonçalves. A cerimónia foi precedida do tradicional porto de honra.

Esta reportagem tinha como objetivo captar a vivência diária dos cidadãos PALOP alojados no Regimento de Transmissões.



PROCISSÃO DE NOSSA SENHORA DA GLÓRIA

Realizou-se no dia 08 de setembro de 2013, a procissão da nossa Senhora da Glória. Esta procissão teve início na Igreja da Graça e deslocou-se para a capela de Nossa Senhora da Glória.

O Regimento de Transmissões, enquanto elemento representativo da Freguesia da Graça, participou nesta cerimónia, com uma representação do Comando da Unidade e quatro praças.



REPORTAGEM TELEVISIVA

Realizou-se no dia 11 de setembro de 2013, a visita de uma equipa de reportagem da RTP com vista à realização de uma reportagem televisiva.

ANTIGOS COMANDANTES

Comandaram o Batalhão de Telegrafistas:



COR Eng
Artur Arsénio Oliveira Moreira
13Jul39 – 26Mai41



TCOR Eng
João Alegria Santos Calado
03Jun41 – 09Dec44



TCOR Eng
Vergílio António F. Quaresma
10Dec44 – 18Mar46



TCOR Eng
Flávio José Álvares dos Santos
19Mar46 – 30Nov48



TCOR Eng
António Nunes Freire
01Dec48 – 22Ago50



TCOR Eng
Artur Quintino Rogado
23Ago50 – 06Out51

Chefiaram o Serviço de Telecomunicações:



TCOR Eng
Jorge César Oom
07Out51 – 10Fev53



TCOR Eng
Mário Santos Risques Pereira
27Fev53 – 29Abr54



TCOR Eng
Manuel Braz Martins
30Abr54 – 14Abr55



TCOR Eng
Victor Francisco Sousa Franco
04Mai55 – 01Jul57



COR Eng
Eduardo Jorge Gomes da Silva
09Jul57 – 27Dec60



TCOR Eng
Jorge Luís Tedeschi Seabra
02Fev61 – 29Jun61



COR Eng
Eduardo Jorge Gomes da Silva
30Jun61 – 23Out62



TCOR Eng
Mário Pinto Fonseca Leitão
24Out62 – 06Jan66



TCOR Eng
Vasco Guilherme Castro Neves
07Jan66 – 09Mai70

Comandaram a Escola Prática de Transmissões:



COR Tm (Eng)
José Francisco Fernandes Basto
10Mai70 – 06Mar72



COR Tm (Eng)
José Sacadura Corte Real
07Mar72 – 28Jun74



COR Tm (Eng)
Gonçalo Nuno Sanches da Gama
29Jun74 – 08Out74



COR Tm (Eng)
António Eduardo Mateus da Silva
09Out74 – 17Nov74



COR Tm (Eng)
António Avelino Pereira Pinto
18Nov74 – 24Mar75



TCOR Tm (Eng)
Carlos Alberto Borges do Rego Falcão
25Mar75 – 03Dec75



COR Tm (Eng)
Francisco José Pinto Correia
04Dec75 - 28Jun76



COR Tm (Eng)
António Luís Pedroso Lima
06Out76 – 31Jan77

Comandaram o Regimento de Transmissões:



COR Tm (Eng)
António Luís Pedroso Lima
01Fev77 – 11Abr78



COR Tm (Eng)
Fernando Eduardo Tinoco Barradas
12Abr78 – 23Set79



COR Tm (Eng)
João Carlos Araújo Geraldès
24Set79 – 28Dec80



COR Tm (Eng)
Mário Manuel Pinto dos Santos
29Dec80 – 14Out84



COR Tm (Eng)
Manuel da Cruz Fernandes
15Out84 – 13Jun89



COR Tm (Eng)
João Manuel Maia de Freitas
14Jun89 – 16Jul92



COR Tm (Eng)
Francisco José F Bastos Moreira
16Jul92 – 10Jul95



COR Tm (Eng)
Joaquim Armando Ferreira da Silva
19Jul95 – 15Jun98



COR Tm (Eng)
António João Mousinho dos Santos
15Jun98 – 26Jun00



COR Tm (Eng)
José Ribeirinha Diniz da Costa
26Jun00 – 19Ago02



COR Tm (Eng)
Edorindo dos Santos Ferreira
21Ago02 – 17Fev04



COR Tm (Eng)
José António Henriques Dinis
30Mar04 – 15Fev06



TCOR Tm
António J. Caessa Alves do Sacramento
15Fev06 – 28Ago06



COR Tm (Eng)
Henrique José da Silva Castanheira Macedo
29Ago06 a 29Set08



COR Tm (Eng)
Nelson Martins Viegas Pires
30Set08 – 28Set10



COR Tm
Francisco José Bento Soares
29Set10-19Set12

SINOPSE HISTÓRICA

1810 – Criação do Corpo Telegráfico, que constitui a origem dos Telegrafistas Militares.

1873 – Origem do Serviço Militar a 17 de Setembro.

1880 – Instalação dos pombais militares.

1884 – Criação do Regimento de Engenharia, no aquartelamento da Cruz dos quatro Caminhos, com três Batalhões, um deles misto, fazendo parte deste uma Companhia de telegrafistas de Campanha.

1901 – Criação da primeira Unidade de Guarnição, Companhia de Telegrafistas de Praça, apoiando a Inspeção do Serviço Telegráfico Militar.

1911 – A reorganização do Exército cria um grupo de Companhias de Telegrafistas a duas Companhias e uma Companhia de Telegrafistas sem Fios.

1913 – Muda a designação para Batalhão de Telegrafistas de Campanha (Quartel da Ajuda) com duas Companhias de Telegrafistas uma de Rádio Telegrafistas e uma Companhia de Condutores.

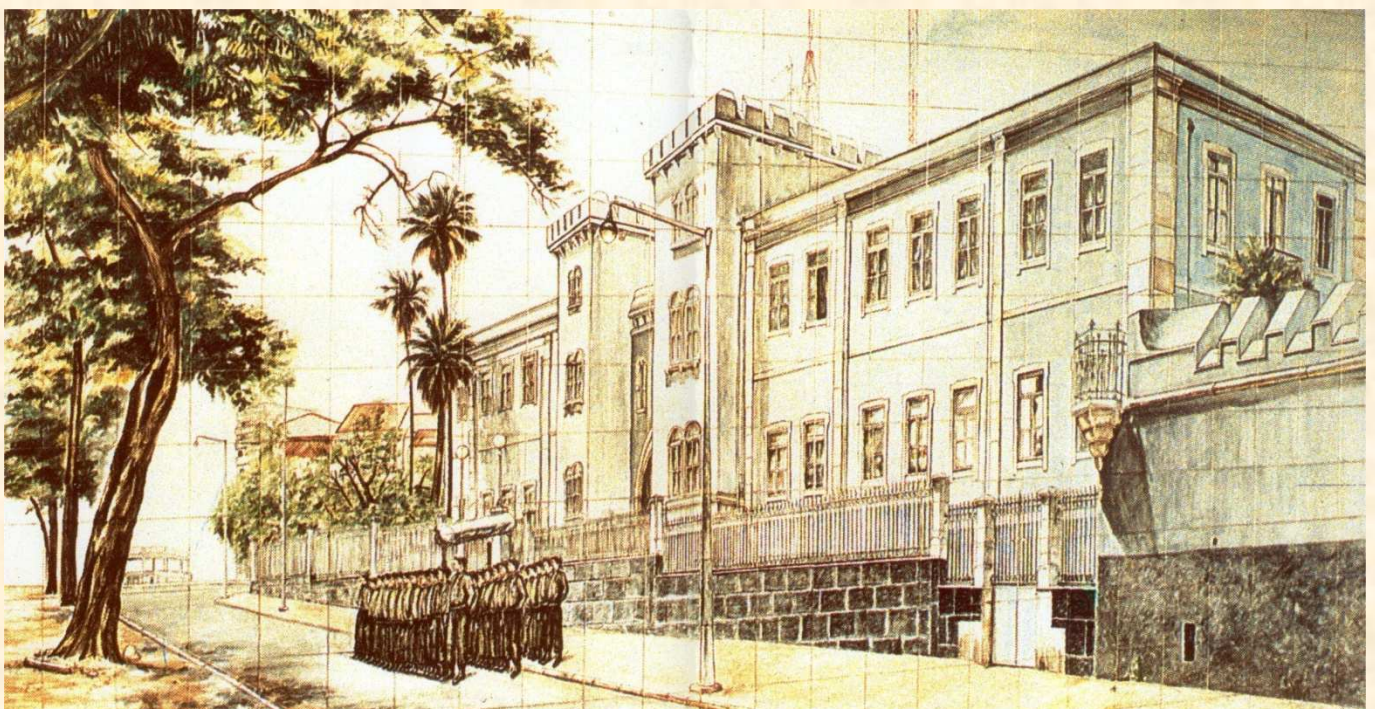
1925 – Por extinção do Batalhão de Telegrafistas de Campanha, criação do Batalhão de Telegrafistas mantendo as mesmas Companhias.

1937 – O Regimento de Telegrafistas é substituído pelo Batalhão de Telegrafistas.

1951 – É criado o Serviço de Telecomunicações Militares (STM), que é assegurado pelo Batalhão de Telegrafistas, mantendo-se no aquartelamento da Cruz dos Quatro Caminhos.

1970 – É criada a Arma de Transmissões, destacando-se da Arma de Engenharia as tropas do Quartel da Cruz dos Quatro Caminhos, sendo criada neste aquartelamento a Escola Prática de transmissões, mantendo adstrito o STM.

1977 – A Escola Prática de Transmissões passa a designar-se Regimento de Transmissões, mantendo adstrito o STM.



Hino das Transmissões

COR TM Alcide D'Oliveira

INTRODUÇÃO



CORO



