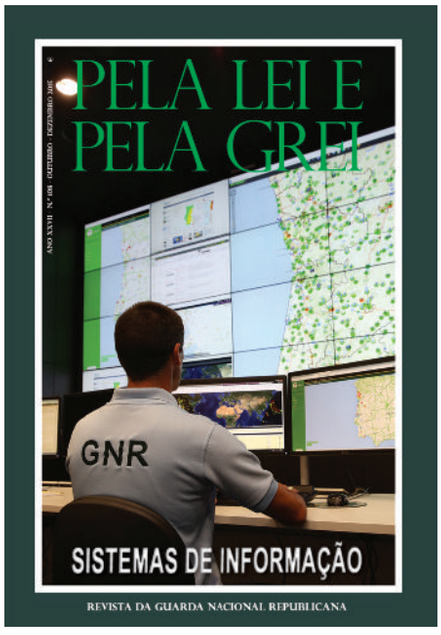
SUMÁRIO



Centro de Comando e Controlo Operacional da Guarda

Ficha Técnica

Comando-Geral da GNR, Largo do Carmo - 1200-092 Lisboa; Tel.: 213217354/294 — Fax 213217159;
E-mail geral: *revista@gnr.pt;*
Diretor: Bartolomeu Nuno de Guanilho da Costa Cabral, Coronel de Cavalaria (Res) **I Chefe da Divisão Revista:** Carlos Manuel Pona Pinto Carreira, Coronel de Administração Militar **I E-mail:** *revista.direccao@gnr.pt* **I Redação:** Fernando Custódio Borges, Cabo-Chefe de Cavalaria; Cláudio Alexandre, Guarda-Principal de Infantaria **I Serviços Administrativos:** Carla Almeida, Cabo de Infantaria; José Rasteiro, Guarda-Principal de Infantaria **I Revisão Ortográfica:** Vasco Zacarias, Cabo de Infantaria **I Fotografia:** Arquivo da Revista, Autores e Secção de Audiovisuais da GNR **I Execução Gráfica:** Gráfica/GNR. **I Tiragem:** 4.400 Exemplares. Depósito Legal N.º 26875/89. ISSN: 1645-9253. Preço Capa: € 1,20; **Assinatura Anual**: € 6,00; Ano XXVII - N.º 108 — outubro - dezembro de 2015. Publicação Trimestral.

No ano de 2012 entraram em vigor as normas constantes do Acordo Ortográfico. A Revista da Guarda, atendendo aos muitos artigos em carteira e às opções dos seus autores vai progressivamente implementando as novas normas, coexistindo as duas formas de escrita. Apelamos, por isso, à compreensão dos nossos leitores.


GNR

Mensagem de Natal

Oficiais, Sargentos, Guardas e Funcionários Civis da Guarda Nacional Republicana

Nesta época festiva do Natal, dirijo-me a todos os militares e civis que servem Portugal na Guarda Nacional Republicana, exprimindo a minha consideração e respeito pela entrega, abnegação e profissionalismo que têm demonstrado no exemplar cumprimento da nobre missão que nos está confiada, garantir a segurança de pessoas e bens.

As celebrações associadas ao Natal convocam à união da família e amigos, favorecendo os valores da amizade e da camaradagem, num ambiente de paz, harmonia e fraternidade que reforça a solidariedade e a partilha.

É um tempo em que estar privado da convivência dos que nos são próximos, nos afeta, naturalmente, de uma forma mais especial. Realço, por isso, os que neste período estarão empenhados em missão de serviço, em território nacional e no estrangeiro, cumprindo o seu dever para que outros possam viver em segurança. A estes militares aqui deixo uma palavra de vigoroso incentivo, apreço e especial consideração.

O ano de 2015, ficou marcado por um árduo e intenso trabalho, num contexto social e económico exigente. Contudo, soubemos enfrentar os desafios e as exigências acrescidas que se colocaram ao nosso País, com os consequentes impactos organizacionais, com reflexos, nos homens e mulheres que diariamente dão o melhor de si, em prol do bem comum. Pelo que, sob todas as circunstâncias, expresso o meu profundo reconhecimento.

A Guarda soube estar à altura das suas responsabilidades, deu resposta pronta e qualificada, contribuindo decisivamente para o ambiente de paz e tranquilidade social, na preservação dos valores que nos caracterizam. Destaco que, não obstante as contingências vivenciadas, registámos um assinalável esforço de concretização na modernização de infraestruturas e meios, indiciadores da modernidade de atuação e proximidade do cidadão que almejamos.

O ano de 2016 certamente prosseguirá na continuidade modernativa e na adequação, concorrendo para uma procura de superação dos desafios que o futuro nos apresentará, dentro de um quadro de novas realidades socioeconómicas e estímulos para a melhoria, na construção de uma GNR, Humana, Próxima e de Confiança.

O Novo Ano que se anuncia será, certamente, desafiador, de árduo trabalho, mas também de esperança e de confirmação da Guarda como uma força de segurança moderna, apta e eficaz. Continuaremos prontos para o desenvolvimento dos trabalhos de revisão dos diplomas estruturantes para a GNR, permitindo a sua melhor adequação a um ambiente de segurança com complexidade e exigência crescentes, na defesa dos interesses da Guarda e dos seus militares e civis.

Neste segundo Natal como Comandante-Geral da Guarda Nacional Republicana, homenageio todos os militares e civis, no ativo, na reserva e na reforma, expressando votos de um Santo e Feliz Natal e de um Próspero Ano Novo, extensível às respetivas famílias.

Lisboa, Carmo, 1 dezembro de 2015
O Comandante-Geral

Manuel Mateus Costa da Silva Couto
Tenente-General

Referências Elogiosas

Ao Comando da Guarda chegou uma missiva que a seguir se transcreve:

"Na sequência dos encontros mensais dos "AMIGOS DO DECALITRO", teve lugar a 27 de maio do corrente ano, uma deslocação ao Comando-Geral da Guarda, de 35 elementos desse grupo.
Servir a Guarda e não conhecer a casa mãe, não devia fazer parte da carreira de nenhum militar, mas as circunstâncias de serviço, de colocação e de carreira, podem levar a que isso aconteça. Havendo militares no grupo a quem isso aconteceu, foi mais uma razão para agendar esta visita.
E em boa hora se tomou essa decisão, pois até quem já tinha estado naquele ancestral edifício ficou a conhecê-lo melhor e ficou a saber onde se passaram muitos momentos marcantes da história de Portugal, o mais recente do conhecimento e participação de tantos Portugueses ainda vivos, "Revolução de Abril 74".
Chegados pelas 11h00, logo fomos encaminhados para o museu, onde, desde o patrono Dom Nuno Álvares Pereira, viajamos por mais de seis séculos de história dentro dos quais a GNR e suas antecessoras, onde podemos observar um relicário de objetos do quotidiano da Guarda, principalmente ao nível de fardamento, armamento, veículos de duas rodas e mobiliário, estando este fielmente exposto ao nível do Posto Territorial, com o qual eu contactei quando em 04AG080 cheguei à Guarda e que constitui um quadro valioso aos que agora chegam e posteriormente irão chegar.
Seguiu-se o salão nobre onde estão patentes as fotos de todos aqueles que comandaram os destinos da GNR desde a sua fundação até aos dias de hoje, espaço onde ocorrem momentos de natural importância da e para a Guarda.
Seguiu-se a varanda do Quartel, magnífico miradouro sobre a cidade de Lisboa, onde não nos cansamos de observar o que nos rodeia e onde, se a imaginação nos permitir, recuando na história, Dom Nuno terá admirado essa beleza de outrora.
O almoço convívio decorreu no refeitório dos Guardas, dentro do ambiente normal do que é o encontro mensal dos amigos do decalitro, tendo durante todo o tempo de estadia no quartel havido diversos reencontros entre militares que se cruzaram em variados pontos do dispositivo, o que se traduziu em mais um ponto importante desta visita.
Pelas 16h00 iniciámos o regresso ao nosso Alentejo.
Queremos deixar um grande obrigado:
Ao SAJ Miguel que desde a primeira hora esteve ao nosso dispor para tornar possível esta visita e nos acompanhou e informou incondicionalmente.
Ao TENCOR Nuno Andrade pela esplêndida exposição oral sobre o Convento/Quartel do Carmo, a sua história, a importância nos momentos de soberania do País e o 25 de Abril.
Á GUARDA Marta Pereira Pela excelente informação durante a visita guiada ao museu.

Ao Comando da Guarda chegou uma missiva de uma Associação que a seguir se transcreve:

"O Papeis & Letras - Associação de Apoio a Crianças e Jovens, vem por este meio louvar os dois agentes que no passado sábado, dia 30 de maio de 2015, pelas cerca de 19 horas, acederam a prestar auxilio ao nosso autocarro acidentado com 49 crianças lá dentro, situação essa que passo a citar:
O autocarro em que nós seguíamos, vindos do Slide & Splash em Lagoa e em direção a Lisboa, rebentou um pneu e foi a muito custo que o motorista conseguiu controlar o autocarro, autocarro esse que ainda se arrastou por alguns metros até conseguir parar. Minutos depois parou logo uma viatura da GNR com dois agentes, Agente Sousa e Agente Bibiu, que prontamente se inteiraram da ocorrência e no meio dos nervos das adultas e algumas crianças assustadas, foram incansáveis em minimizar o problema, inclusive com uma grande preocupação referente às crianças, exigindo ao senhor motorista que abrisse todas as portas e janelas possíveis, pois as crianças estavam dentro do autocarro. Ajudaram também a controlar o trânsito assim como a levar as nossas crianças, uma a uma, a fazer as suas necessidades em segurança, visto que o local onde estávamos era muito perigoso.
Vimos desta forma reforçar a nossa eterna gratidão aos Agentes Sousa e Bibiu, que nesta situação complicada foram de uma calma, simpatia e profissionalismo inquestionáveis.
Um BEM HAJA aos senhores Agentes da GNR
Com os melhores cumprimentos"

O Século XX poderá ser definido ou lembrado conceptualmente de diversas formas, mas é, sem dúvida, o período da história do advento da Era da Informação. Sempre em crescendo, a partir daquela época, a informação começou a fluir com uma densidade inaudita dando, no entanto, origem a um mundo assimetricamente globalizado, acentuando a geopolítica da inclusão-exclusão. Assistimos a invenções fabulosas destinadas à transmissão de dados. Fomos confrontados com meios de comunicação de massa, e estamos interligados por uma grande rede de comunicação que é a *Internet*, o que tem obrigado o ser humano a lidar com um crescimento exponencial do volume de dados disponíveis, i. e., com um superavit de informação. Ficámos mais próximos, reduziram-se distâncias e passámos a ter acesso a mais dados.

Tornou-se necessário joeirar a informação disponível, de modo a, numa analítica transdisciplinar, escalpelizar factores do passado, para tornar inteligível o presente e, primordialmente, antever, quanto possível, escatologicamente o futuro – a cenarização e a prospectiva assentaram arraiais!

A designação Sistemas de Informação passou a fazer parte do léxico das organizações. Para Laudon, "*um sistema de informação pode ser definido como um conjunto de componentes interrelacionados trabalhando juntos para colectar, recuperar, processar, armazenar e distribuir informações, com a finalidade de facilitar o planeamento, o controle, a coordenação, a análise e o processo decisório em organizações".*

Num Sistema de Informação bem gizado, todos os intervenientes, para além de trabalharem para um objectivo comum, como acontece em qualquer sistema, tornam o fluxo das informações mais confiável e menos burocrático, aumentando a integridade e veracidade da informação. Deste modo, conseguem-se reduções nos custos operacionais e administrativos, associados a ganhos de produtividade, a uma maior estabilidade e a mais segurança no acesso à informação. Desta forma, criam-se condições para os decisores estarem habilitados com informações de boa qualidade, essenciais para uma boa tomada de decisão.

Actualmente, um Sistema de Informação de grande dimensão só poderá sobreviver se estiver informatizado, obrigando à interacção da componente humana com as Tecnologias de Informação.

Consciente da evolução operada na sociedade e ciente da importância de possuir Sistemas de Informação adequados, a Guarda, ao querer proporcionar melhor e mais segurança, decidiu criar um órgão na sua estrutura de Comando, o Grupo de Trabalho para as Tecnologias de Sistemas de Informação da GNR-(GT-TSI), agregador das atribuições dos actuais órgãos na área das Tecnologias de Sistemas de Informação, funcionando na dependência directa do Comandante Operacional, com a missão de liderar o processo de, com recurso às novas tecnologias, incrementar a eficiência e eficácia, racionalizar os recursos humanos e materiais, garantindo também uma maior segurança aos seus militares no terreno e prestando um melhor serviço aos portugueses.

Antes de convidar os nossos leitores a tomarem conhecimento da mudança e inovação em curso nos Sistemas de Informação da Guarda, tema de capa neste número, não poderei deixar de formular os votos de um Santo Natal e de um Feliz Ano Novo a todos os que nos dão a honra de lerem a Revista *Pela Lei e Pela Grei*.

Quartel do Carmo, Lisboa, 17 de Dezembro de 2015

O Director da Revista

Bartolomeu Nuno de Guanilho da Costa Cabral
Coronel de Cavalaria (Res)

Aniversários

Comando Territorial de Santarém

O Comando Territorial de Santarém comemorou, no passado dia 15 de outubro, o seu sétimo aniversário. Nesta data, que evoca a chegada pela primeira vez da GNR a terras "Scalabitanas" (13OUT1912), em que a 4.ª Companhia do Batalhão n.º 2 se instalou inicialmente, no edifício da Mitra (atual Caixa Geral de Depósitos), importava celebrar esse evento através de uma cerimónia que dignificasse quer a Guarda, quer o Comando Territorial de Santarém, recordando as suas ações e marcas históricas e vincando o espírito de corpo, o orgulho e a dedicação dos militares por servirem na Unidade. A cerimónia militar realizada na cidade de Almeirim, no jardim em frente ao Posto Territorial, foi presidida pelo Exmo. Comandante do Comando Operacional da GNR, Major-General Botelho Miguel e contou com a presença de diversas entidades civis e militares do distrito, designadamente, com o excelentíssimo Senhor Doutor Pedro Miguel César Ribeiro, Presidente da Câmara Municipal de Almeirim.

As forças em parada foram constituídas pela Banda de Música e Fanfarra da Unidade de Segurança e Honras de Estado da GNR, e por forças compostas pelas diversas valências do Comando, nomeadamente, a cinotécnica, pelotões de infantaria, vertentes ciclo, trânsito, intervenção, náutica, proteção da natureza e ambiente e programas especiais, sob o comando do Major de Cavalaria Pinto Reis.

No âmbito da cerimónia militar, foi proferida uma alocução pelo Comandante da Unidade, Coronel de Infantaria Nuno Sanfona Paulino e outra pelo Exmo. Comandante do Comando Operacional da GNR. Foram ainda impostas condecorações aos militares deste Comando Territorial agraciados durante o último ano. A cerimónia continuou com uma homenagem aos militares falecidos que serviram na Unidade, na presença do Sr. Coronel Capelão Agostinho Freitas, Chefe do Serviço de Assistência Religiosa da GNR e terminou com o desfile das forças em parada, em continência ao Exmo. Comandante do Comando Operacional da GNR.

Nos restantes quarteis do dispositivo foram realizadas pequenas cerimónias, que contaram com a presença de todos os militares disponíveis, onde foi lida a mensagem do Exmo. Comandante da Unidade.

Na sua alocução, o Comandante da Unidade destacou os indicadores da atividade operacional desenvolvida ao longo do último ano, como sendo muito positivos e esclarecedores do empenhamento e dedicação dos militares da Unidade e

que contribuíram para o lema da Unidade, "Sempre Enobrecido Scalabicastro".

Após a alocução do Comandante da Unidade, o Exmo. Comandante Operacional da GNR proferiu algumas palavras, começando por se dirigir ao Presidente da Câmara Municipal de Almeirim e na pessoa deste, a todos os habitantes da cidade, destacando a excelência de uma cidade marcada pela história, onde a sabedoria antiga comunga com a atual e a importância da mesma para a economia do país, sublinhando o contributo de 103 anos da GNR para a história daquela cidade. Agradeceu a todas as restantes entidades, realçando que a partilha deste dia com personalidades tão ilustres e representativas é motivo de honra e orgulho para os militares que servem a Guarda. Seguidamente, dirigiu-se aos Oficiais, Sargentos, Guardas e funcionários Civis do Comando, afirmando que a celebração do Dia da Unidade é uma forma de recordar os que nos precederam. Destacou a sinergia de esforços entre a Guarda e as instituições do poder local, como proveito de todos, que tem contribuído para a produção da imagem de uma região tranquila e segura, destacando ainda, os excelentes resultados alcançados, que são o esforço de todos e que simbolizam o que a Guarda tem de melhor, homens e mulheres, que trabalham arduamente, em prol do bem comum para garantir a segurança e a tranquilidade das pessoas. Por fim, incitou os militares para que nunca deixem de ter presente a sua generosidade, dinamismo e entrega, mas também a capacidade e competência, incitando a força a manter uma Guarda "Humana Próxima e de Confiança".

Após esta cerimónia, foi realizada uma outra nas instalações do Posto Territorial de Almeirim para entrega de uma viatura cedida em regime de comodato pela Câmara Municipal de Almeirim, e para utilização daquele Posto no policiamento dos campos agrícolas da localidade.

O senhor Presidente da Câmara Municipal de Almeirim proferiu umas breves palavras alusivas ao ato e de seguida, a viatura foi benzida pelo Sr. Capelão da GNR, em conjunto com o Pároco de Almeirim, terminando com a entrega simbólica da chave ao Comandante do Posto Territorial de Almeirim, 2.º Sargento Pereira.

Unidade de Controlo Costeiro

No dia 23 de outubro, a Unidade de Controlo Costeiro comemorou o seu 7.º Aniversário.

Para assinalar este evento foi realizada, na manhã do dia 22 de outubro, uma missa de sufrágio pelos militares da UCC falecidos, e no dia 23 de outubro, teve lugar na Doca do Espanhol, em Alcântara, a cerimónia principal.

A celebração desta efeméride compreendeu um conjunto de atividades de caráter militar e religioso, singelas, mas com um significado especial militar, tanto na vida interna da UCC, como na imagem que dela se projeta para o exterior.

Estas comemorações, assinaladas em todas as subunidades, iniciaram-se pelas 08H00 com o içar da bandeira nacional e prosseguiram às 11H00 com uma parada militar presidida por Sua Ex.ª, a Ministra da Administração Interna, Prof.ª Dr.ª Anabela Miranda Rodrigues, tendo as forças em parada sido constituídas num Batalhão composto por uma Companhia terrestre e uma Companhia marítima.

Estiveram presentes na cerimónia o Exmo. Comandante-Geral da Guarda Nacional Republicana, Tenente-General Manuel Mateus Costa da Silva Couto, demais altas entidades militares e civis convidadas e Oficiais Generais e Comandantes de Unidades e Órgãos Superiores de Comando e Direção da Guarda.

A cerimónia militar iniciou-se com apresentação da formatura à alta entidade, seguida de integração do Estandarte Nacional, alocução do Comandante da UCC, alocução de S.Exª, a Ministra da Administração Interna, imposição de condecorações e homenagem aos militares falecidos.

PELA LEI E PELA GREI

Da cerimónia salienta-se a homenagem aos mortos, designadamente, evocando os dois militares da Unidade falecidos ainda ao serviço, no decorrer do último ano.

Os discursos da Exma. Ministra da Administração Interna e do Exmo. Comandante da UCC, atendendo aos seus conteúdos e mensagens, mereceram atenção por parte de todas as entidades presentes, assim como dos militares, já que foi destacado o relevante contributo da Unidade na fiscalização das pescas, no controlo do narcotráfico e ainda o expressivo desempenho no plano internacional, na salvaguarda de vidas no mar.

As forças em parada, sob o comando do Tenente-Coronel de Infantaria João Nascimento, desfilaram com brio, encerrando a cerimónia militar.

De seguida, todos os convidados presentes na cerimónia puderam apreciar a apresentação de um novo diaporama sobre o SIVICC (Sistema Integrado de Vigilância e Controlo Costeiro) que, de uma forma dinâmica e explícita, sintetiza a operação do sistema e o seu contributo para a segurança da fronteira externa da União Europeia.

Em súmula, foi um dia festivo, importante para a Guarda e em particular para a UCC, revestindo-se de extrema dignidade e sobriedade.

Comando Territorial de Aveiro

O Comando Territorial de Aveiro comemorou no dia 10 de novembro de 2015, o seu 7.º aniversário. Cumpriu-se, assim, uma tradição que se reveste de particular relevância por contribuir para o reforço da coesão e do espirito de corpo.

A celebração decorreu na parada General Tamagnini, perante um conjunto distinto de entidades militares, civis e religiosas do distrito de Aveiro, de onde se realça a presença da grande parte dos presidentes e edis representantes do poder local.

A cerimónia foi presidida pelo Exmo. 2.º Comandante-Geral da GNR, Major-General Luis Filipe Tavares Nunes, a quem foram prestadas as honras militares regulamentares.

As forças em parada foram constituídas pela Banda Marcial e Fanfarra da Unidade de Segurança e Honras do Estado, por duas companhias operacionais e por um bloco motorizado representativo de todas as valências do Comando Territorial de Aveiro.

Após a integração do Estandarte Nacional na formatura, o Comandante em suplência, do Comando Territorial de Aveiro, Tenente-Coronel de Infantaria Nélson Manuel Machado Couto e o Exmo. 2.º Comandante-Geral, Major-General Luís Filipe Tavares Nunes proferiram alocuções alusivas à cerimónia.

De seguida, procedeu-se à imposição de condecorações a militares e civis do Comando que foram agraciados no último ano, sucedendo-se a homenagem aos militares mortos em serviço.

Em apoteose, as forças em parada desfilaram em continência à alta entidade que presidiu à cerimónia, dando-se, assim, por finalizadas as comemorações alusivas ao dia festivo da Unidade.

GNR de Loulé apreende pólen de haxixe

Durante a madrugada do dia 01 de outubro de 2015, militares do Núcleo de Investigação Criminal (NIC) de Loulé Destacamento Territorial da Guarda Nacional Republicana (GNR) detiveram três cidadãos do sexo masculino, com idades compreendidas entre os 39 e os 51 anos, indiciados pela prática do crime de tráfico de estupefacientes. Cerca das 05h00, a presença e movimentações duvidosas de três cidadãos que se encontravam na estação de serviço de Loulé da Autoestrada A22, sentido Faro-Albufeira, levantou suspeitas que levaram um popular a solicitar a presença da GNR, tendo sido acionada para o local uma patrulha do Posto Territorial da GNR de Loulé e militares do NIC daquele Destacamento. Após avaliação da situação, a atitude e postura demonstrada pelos indivíduos adensou as suspeitas relativamente ao propósito da presença dos mesmos naquele local, surgindo de imediato indícios de que poderíamos estar perante cidadãos que se encontravam a efetuar transporte de estupefaciente no interior do corpo, vulgo "mulas de droga." As diligências entretanto adotadas, nomeadamente, transporte dos indivíduos ao Hospital de Faro, permitiram confirmar que dois dos suspeitos tinham estupefaciente nos intestinos, tendo entretanto expulsado pólen de haxixe, acondicionado sob a forma de bolotas, suficiente para 21250 doses individuais.

Transporte de Órgãos Um serviço de excelência

A Guarda Nacional Republicana (GNR) desempenha desde 1994, através da sua valência de trânsito, a missão de transporte de órgãos entre vários centros hospitalares, em todo o território nacional.
Nesta missão, a GNR é contactada pela Unidade de Saúde que detém o órgão a ser transportado, despoletando de imediato uma patrulha de trânsito que se desloca até esta, transportando o órgão nas exigidas condições térmicas até ao seu destino, ou seja, até ao bloco operatório da unidade hospitalar requisitante. Dos 233 transportes de órgãos realizados desde o início do ano, a GNR empenhou 465 militares, percorreu 38.717 quilómetros e registou como os três distritos com mais transportes requisitados: Lisboa - 62; Setúbal - 40; e Coimbra - 31.
A qualidade e segurança da transplantação de órgãos depende do tempo necessário para o seu transporte, competindo assim à GNR e em respeito das condições de segurança, chegar ao destino no menor tempo possível, contribuindo, deste modo, para o salvamento de mais uma vida.

Presença da Guarda em Marrocos no 8.º Festival do Cavalo

A Guarda Nacional Republicana esteve presente, de 13 a 18 de outubro, na 8.ª edição do "Salão do Cavalo" em El Jadida, Marrocos, evento que teve Portugal como convidado de honra. A Reprise e a Charanga da Guarda Nacional Republicana realizaram diversas demonstrações nesse período, tendo atuado no dia da abertura oficial a 12 de outubro, presidido pelo Sereníssimo Príncipe de Marrocos, Sua Alteza Moulay Rachid, onde esteve presente, para além de outras individualidades nacionais, a ministra da Agricultura e do Mar, Professora Doutora Assunção Cristas. Em 13 de outubro, no decorrer da abertura oficial ao público, a Reprise e a Charanga voltaram a atuar, estando patente, no espaço dedicado ao certame, o património equestre português, sublinhando deste modo, a cooperação entre os dois países nesta temática.

Operação Guadiana

A Unidade de Ação Fiscal (UAF) da GNR e a Direção de Finanças de Beja, da Autoridade Tributária (AT), apoiados pela Direção de Serviços de Investigação de Fraude e Ações Especiais da AT, pela Unidade de Intervenção da GNR e pelos Comandos Territoriais de Faro, Beja e Setúbal, deram cumprimento no dia 20 de outubro, a 15 mandados de busca e apreensão.

A operação decorreu em várias localidades disseminadas pelos distritos de Lisboa, Setúbal, Beja e Faro, e foi o resultado de 13 meses de investigação conduzidos para a consubstanciação dos crimes de fraude fiscal qualificada, burla tributária e frustração de créditos e branqueamento de capitais. Na sequência das referidas buscas foram constituídos 13 arguidos (cinco pessoas singulares e oito pessoas coletivas) e apreendidos vários suportes de armazenamento de dados digitais (*CPU*, discos rígidos, etc.) e documentação diversa, que permitem apurar a obtenção e dissimulação de vantagens patrimoniais ilícitas na ordem das várias centenas de milhares de euros.

Curso CEPOL

No âmbito das atividades da Academia Europeia de Polícia (CEPOL), a Escola da Guarda organizou, de 09 a 20 de novembro de 2015, o Curso CEPOL "*EU CSDP Police Command and Planning Course*", tendo a cerimónia de encerramento sido presidida pelo Exmo 2.º Comandante-Geral da Guarda, Major-General Luís Filipe Tavares Nunes. Este curso teve a finalidade de formar 26 oficiais superiores de polícia, provenientes de 22 Estados-Membros da União Europeia, com vista a desenvolver as competências de comando e controlo exercido em missões europeias de gestão civil de crises. Durante o curso, oradores nacionais e internacionais ministraram palestras, versando as seguintes temáticas:

- Gestão civil de crises: planeamento estratégico e o processo de decisão;
- Gestão civil de crises: o mandato da missão; Liderança e a diversidade multicultural; e Segurança e os modelos de segurança.

1.ª equipa cinotécnica de deteção de venenos em Portugal

A Guarda Nacional Republicana participa, até dezembro de 2018, no projeto "*LIFE Imperial*: Conservação da Águia-Imperial ibérica em Portugal", com a criação da 1.ª equipa cinotécnica de deteção de venenos, pioneira em Portugal.

O projeto tem como objetivo promover o aumento da população da Águia-Imperial ibérica em Portugal, sétima ave de rapina mais ameaçada do mundo pela ação humana, nomeadamente, pelo abate a tiro e envenenamento, sendo este último método uma das principais causas de mortalidade não natural da espécie em Espanha. As três equipas cinotécnicas especializadas na deteção de venenos, criadas neste projeto, incorporam sete cães Pastores Belga *Malinois* e *English Springer Spaniel*, a incorporar no Serviço de Proteção da Natureza e Ambiente da Guarda Nacional Republicana (SEPNA-GNR). Estas equipas tem intervenções previstas nas Zonas de Proteção Especial (ZPE) da Rede Natura 2000 de Castro Verde, Vale do Guadiana, Mourão/Moura/Barrancos e Tejo Internacional, Erges e Pônsul. A criação de binómios detetores de venenos irá aumentar a capacidade de vigia e controlo da ameaça, onde o despiste de casos de envenenamento na natureza será efetuado por patrulhas cinotécnicas regulares, nas áreas de intervenção do projeto que terão um caráter:

- Preventivo: com o intuito de detetar situações de uso ilegal de venenos, nomeadamente, a presença de iscos envenenados. Nestas situações, a utilização de cães permite fiscalizar áreas muito extensas e, por vezes, de difícil acesso;
- Reativo: com o intuito de verificar situações com cadáveres ou animais selvagens ou domésticos, com indícios de envenenamento;
- Criminal: facilitando a abertura de processos criminais com uma maior quantidade e qualidade de provas obtidas, num processo conduzido pelo mesmo órgão (deteção, recolha e processamento, investigação), aumentando a probabilidade de determinação e culpabilização dos responsáveis.

A este patrulhamento intensivo, concretamente direcionado à proteção da Águia-Imperial ibérica, está associado um efeito preventivo e dissuasor decorrente desta presença cinotécnica constante e regular, no terreno. O projeto "*LIFE Imperial*" é um projeto coordenado pela Liga para a Proteção da Natureza - LPN e conta com oito beneficiários associados nacionais e espanhóis, entre os quais, a GNR, sendo financiado em 75% por fundos comunitários do programa "*LIFE*" da União Europeia.

Ministra da Administração Interna visita Comando-Geral

A Guarda Nacional Republicana recebeu no dia 14 de dezembro, no Quartel do Carmo, pelas 11:00 horas, a primeira visita Oficial da Exma. Ministra da Administração Interna, Professora Doutora Constança Urbano de Sousa.

Teve como objetivo proporcionar um melhor e mais detalhado conhecimento deste Corpo Especial de Tropas e das suas diversas valências. No decurso da visita foi apresentado um *briefing* sobre a missão e atividade da Guarda, dado a conheçer o novo Centro de Comando e Controlo Operacional da Guarda, terminando com uma exposição estática, representativa dos diversos meios e valências desta Força de Segurança.

Celebração de Natal do Comando-Geral da GNR

Como de costume, no âmbito do almoço de Natal do Comando-Geral da Guarda Nacional Republicana, celebrou-se Missa na basílica dos Mártires. Presidiu o Bispo das Forças Armadas e das Forças de Segurança. O Pe. Agostinho Freitas, Capelão Adjunto, concelebrou.

Na homilia, D. Manuel Linda acentuou dois pontos: o sentido da familiaridade que esta época transmite e o Natal como um dado da nossa cultura. Quanto ao primeiro aspecto, afirmou que o Natal nos atrai porque nos apresenta realidades a que estamos habituados e que nos dizem muito: uma mãe, um pai e um bebé. É este sentido de família que deve ser expandido até à dimensão global, de todo o mundo. Mas não se pode esperar que o mundo seja uma família se, antes, não se constrói familiaridade nos ambientes em que cada um de nós se move. E vincou: "*Da mesma forma que, nas nossas famílias de sangue, nos alegramos ou entristecemos com as alegrias ou tristezas de cada membro e todos se*

preocupam com os que sofrem, assim tem de acontecer na Guarda: precisamos de uma especial sensibilidade para descobrir o que se passa de ânimo ou desânimo, no interior de cada camarada e marcar presença fraterna junto desse irmão, fazendo nossas as suas dificuldades e angústias. Que nas Unidades, Comandos, Destacamentos e Postos, cada militar seja o anjo da guarda do seu camarada".

Quanto à dimensão cultural do Natal, referiu situações em que, por motivos de um falso diálogo inter-religioso ou mal-entendido respeito por outras crenças se chega a proibir a referência ou representação do presépio, criando, assim, um vazio cultural. E assegurou: "*Da mesma forma que, segundo o velho princípio da física, «a natureza tem horror ao vácuo», também na cultura, se negarmos a dimensão religiosa cristã, outras perspectivas virão preencher esse vazio. Mas então, deixaremos de ouvir falar de paz, de amor, de fraternidade, de liberdade, para passarmos a escutar apelos à guerra, à desestabilização social, à imposição de doutrina, ao terrorismo, precisamente em nome de uma qualquer divindade que nos é estranha. A civilização ocidental tem, portanto, de escolher o que deseja*".

A seguir a esta Missa, solenizada pelo Coro da GNR e participada pelo Comandante-Geral, vários Oficiais Generais, Oficiais, Sargentos, Guardas e Civis, decorreu um almoço nas instalações do Carmo, já com a presença da Ministra da Administração Interna e seus Secretários de Estado.

Sistemas de Informação

Os Sistemas de Informação têm uma importância decisiva na satisfação das necessidades de informação de qualquer organização. A Guarda, ao querer proporcionar "mais e melhor segurança", identificou o papel central dos Sistemas de Informação para a consecução daquele objetivo e decidiu materializar o seu peso, através da criação de uma estrutura que tem vindo a revelar-se fundamental na prossecução dos Objetivos Estratégicos da Guarda para o horizonte 2015-2020.

Efetivamente, com o despacho n.º 83/2014 do Exmo. Comandante-Geral, foi criado um órgão na estrutura do Comando da Guarda, agregador das atribuições dos atuais órgãos na área das tecnologias de Sistemas de Informação, a concretizar em futuro processo de revisão orgânica deste corpo especial de tropas.

A funcionar na dependência direta do Comandante Operacional e considerando o papel determinante dos Sistemas de Informação, na satisfação das necessidades de *competitive intelligence* em qualquer organização, designadamente, nas operações, processos e tomada de decisão, com o despacho supracitado, foi constituído o "Grupo de Trabalho para as Tecnologias de Sistemas de Informação na GNR" (GT-TSI).

O GT-TSI tem como missão assegurar a gestão dos projetos transversais na Guarda e a direção, coordenação, controlo, gestão e execução das atividades da Guarda em matéria de sistemas e tecnologias da informação, sendo de revelar as seguintes atribuições:

- Controlo de qualidade, no âmbito do funcionamento, operação e utilização dos sistemas de informação;
- Exercer a autoridade técnica em relação à manutenção das tecnologias de informação;
- Coordenar os projetos, no âmbito dos Sistemas de Informação;
- Acompanhar a gestão de serviços de desenvolvimento de *software*, internamente ou em regime de *outsorcing*.

As principais linhas de orientação estratégica integradas na Estratégia da Guarda 2020, com vista ao cumprimento da missão da Guarda e, em particular, as estratégias parcelares que têm vindo a ser desenvolvidas, das quais se destaca a estratégia para as Tecnologias de Informação e Comunicação, visam incrementar a eficiência, eficácia, racionalizar os recursos humanos e materiais, prestar um melhor serviço ao cidadão e garantir maior segurança aos nossos militares no terreno, princípios vertidos em todas as linhas de ação do Comando Operacional e que têm como elemento agregador e difusor o Centro de Comando e Controlo Operacional.

Com este passo, foram criadas condições para o estabelecimento de um elevado nível de coordenação, com vista a uma maior eficácia e eficiência das atividades inerentes ao quadro de atribuições e missões da Guarda.

Major-General SANTOS CORREIA
Adjunto do Comandante Operacional

Estratégia para as Tecnologias e Sistemas de Informação da Guarda

1 - INTRODUÇÃO

Um elemento crucial para uma instituição de referência é a definição clara, objetiva e inequívoca da sua missão, a qual espelhe a sua forma de atuação, organização, governação e que, de forma resumida, facilite a elaboração de estratégias, expresse a sua própria razão de existência e sintetize os seus principais valores.

Os valores institucionais representam as crenças e convicções dominantes numa organização como a Guarda, enquanto elemento singular no quadro do Sistema de Segurança Nacional, caraterizados pela sua constância temporal, sendo o Conhecimento e a Inovação um dos seus pilares fundamentais. Deste, releva a aquisição de conhecimento como essencial para um "desenvolvimento inteligente", vocacionado para a melhoria da segurança e liberdade dos Cidadãos, promovendo a inovação no desenvolvimento da atividade policial, antecipando ameaças e riscos que comprometam os direitos, liberdades e garantias, constitucionalmente consagrados.

Na prossecução dos Objetivos Estratégicos e operacionalização da visão do Exmo. Tenente-General Comandante-Geral, segundo as Linhas de Orientação Estratégica definidas no documento "ESTRATÉGIA DA GUARDA 2020 - Uma Estratégia de Futuro", ressalta "Modernizar, Inovar e Simplificar" com o escopo de garantir a celeridade e eficiência dos processos, privilegiar o recurso a novas tecnologias de informação e de comunicação, manter a aposta na inovação tecnológica ao serviço da segurança, valorizar a formação dos recursos humanos, desmaterializar processos e simplificar procedimentos, para requalificar os serviços operacional e de apoio, e potenciar maior articulação entre Forças e Serviços de Segurança.

Tendo em conta os desideratos supraidentificados, a legislação e normativo envolventes na área SI/TIC, assim como a visão para cada área de especificidade da Guarda, o Grupo de Trabalho para as Tecnologias e Sistemas de Informação (GTTSI) tem vindo a desenvolver um trabalho prospetivo, no sentido de melhorar a acessibilidade aos SI por parte do militar no terreno, incrementar o apoio à decisão de forma automatizada e transversal a toda a hierarquia e possibilitar o comando e controlo através de uma *common operational picture* ao Comando Superior, assente nas seguintes vertentes:

- Implementação de um novo Centro de Comando e Controlo Operacional (CCCO), com normativo e procedimentos modernos e adaptados;
- Sistema de policiamento vocacionado para *Intelligence-led Policing* e *Evidence Based Policing*, assente na transmissão tempestiva de dados das ocorrências do terreno para as Salas de Situação;
- Reorganização do modelo de governação na área das Tecnologias e Sistemas de Informação.

2 - MEDIDAS NA ÁREA DAS TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO

Tendo em conta o alinhamento entre os valores institucionais da Guarda, as Linhas de Orientação Estratégicas e os Objetivos Estratégicos das TSI, no horizonte 2015-2020, as medidas preconizadas que contribuem para atingir os Objetivos Estratégicos da Guarda, na esfera de competência das tecnologias e sistemas de informação, foram as seguintes:

1 - Melhorar a capacidade integrada de Comando, Coordenação e Controlo articulada com a gestão das áreas de apoio operacional, potenciando os sistemas tecnológicos e de informação, de forma a conduzir com eficácia acrescida, operações aos níveis tático (Comando Territoriais) e tático-operacional (Comando Operacional).

2 - Privilegiar o recurso a novas tecnologias de informação e de comunicação, valorizando a formação dos recursos humanos, desmaterializando atos e simplificando procedimentos, visando requalificar o serviço operacional e de apoio, potenciando uma maior cooperação e articulação entre as Forças e Serviços de Segurança;
3 - Promover a simplificação e racionalização de procedimentos, reforçando a interoperabilidade e conetividade entre os diversos sistemas de informação operacionais e de apoio operacional, que potenciem uma perspetiva agregada da performance institucional;
4 - Incrementar a capacidade de atuação no ciberespaço, garantindo uma resposta integrada da instituição ao fenómeno da cibercriminalidade no mundo real e virtual;
5 - Melhorar os níveis de eficiência operacional, por via da requalificação das infraestruturas e equipamentos (parque automóvel, tecnológico, armamento e equipamentos específicos), assegurando as condições de trabalho adequadas aos profissionais da Guarda.

3 - PLANEAMENTO E IMPLEMENTAÇÃO DE AÇÕES E PROJETOS

Para a afirmação do capital de prestígio que a Guarda granjeia junto dos cidadãos e particularmente, a confirmação do seu estatuto de centro de excelência nas áreas do trânsito, da proteção da natureza e ambiente, da proteção e socorro, da vigilância e controlo costeiro e em áreas emergentes, como as da utilização de vetores aéreos e da cibersegurança, importa que a área das Tecnologias e Sistemas de Informação contribua para planear, aprovar e implementar um conjunto alargado de ações e projetos que garantam melhor qualidade da informação, maior sinplicidade para o utlizador, acrescidas eficácias e eficiências dos sistemas de informação e maior robustez da infraestrutura tecnológica.

Tendo em conta as medidas preconizadas e os objetivos holísticos supracitados, é determinante a identificação de ações e projetos a desenvolver em prol de cada objetivo estratégico, os quais sejam mensuráveis e contribuam da forma mais significativa possível, para "alavancar" o produto final das componentes operacional e dos recursos internos da Guarda.

3.1 - Melhorar a capacidade de Comando, Coordenação e Controlo

- Produzir uma imagem única comum, "a verdade", transversal aos diferentes utilizadores para a mesma situação, de forma a incrementar o rigor da informação disponibilizada pelos SI;
- Assegurar a normalização, qualidade, completude

Alinhamento entre os valores institucionais da Guarda, as Linhas de Orientação Estratégicas e os Objetivos Estratégicos das TSI, no Horizonte 2015-2020.

e precisão da informação, bem como a sua disponibilidade, integridade, rastreabilidade e auditabilidade[1];

- Disponibilizar ao decisor e utilizadores, de forma tempestiva, informação relevante, no formato pretendido, de forma a gerar elevado valor acrescentado;
- Efetuar o levantamento de processos-chave, subprocessos e funções identificados nos âmbitos operacional e de apoio, de forma a implementar os requisitos específicos para cada processo;
- Disponibilizar ferramentas de análise e gestão, adaptáveis aos cenários de utilização, às necessidades do decisor e demais utilizadores;
- Garantir a obtenção de indicadores e dados requeridos para elaboração de planos e relatórios, de forma mais automatizada, com maior coerência, integração e normalização em todo o dispositivo[2];
- Definir três níveis de tratamento de informação policial, através de sistemas de informação distintos, complementares e interoperáveis assentes em:
- Um 1.º nível **(Dados),** correspondente ao registo imediato e sumaríssimo de qualquer tipo de incidente, registando-se apenas dados nucleares (Quando, Onde, Quem, Tipo de incidente, o Quê, e Como) necessários para o processo de decisão e intervenção policial imediato;
- O 2.º nível **(Informação),** englobando a posterior validação e recolha adicional de dados do incidente, tendo em vista potenciar o ciclo de produção de informação;
- O 3.º nível **(Conhecimento)**, assente em ferramentas de *data warehousing*, *data mining/Business Inteligence* e *case management*, de forma a garantir *awareness* e uma elevada capacidade de predizer ameaças, identificar tendências e caraterizar fenómenos criminais.
- Garantir o Sistema Integrado de Informações Operacionais Policiais (SIIOP) como repositório de dados e sistema transacional base, de forma a contribuir para um serviço policial de excelência, através das seguintes ações:
- Incrementar a velocidade e facilidade de acesso, aumentar as funcionalidades disponibilizadas, o *reporting* e as ferramentas de análise, de forma a permitir maior capacidade operacional, no âmbito da prevenção, predição e combate à criminalidade;
- Alargar a rede SIIOP a todo o território nacional e Regiões Autónomas dos Açores e da Madeira, em harmonia com o projeto SAMA;
- Potenciar a interoperabilidade do SIIOP com outros sistemas de informação internos e externos à GNR.
- Suportar um modelo de policiamento orientado aos fenómenos criminais e em "comunidades de prática" policiais (*Evidence-based policing*), assente em ferramentas de *awareness*, de síntese e transmi- ssão de conhecimento.
- Redefinir o modelo de atuação operacional, valorizando o trabalho de registo, encaminhamento e acompanhamento da ocorrência pela Sala de Situação (SSit), garantindo maior proteção e mitigação do risco para o Patrulheiro, através dos seguintes procedimentos:
- Recorrer ao sistema SG2S para o serviço de *dispatch* de meios e o acompanhamento da situação, sendo a introdução de dados e análise de risco efetuada na SSit, a partir da comunicação via rádio pelo Patrulheiro;
- Efetuar a validação da informação sobre a ocorrência após a chegada ao Posto do Pa-

Imagem única comum, "a verdade", tempestiva e relevante

Disponibilidade, integridade, rastreabilidade e auditabilidade

Sistema Integrado de Informações Operacionais Policiais (SIIOP) como repositório de dados

[1] - Incluindo a existente/derivada de sistemas legados.
[2] - Obtenção de informação a fornecer a entidades internas e externas, como e.g. o denominado Modelo 262.

Assinatura eletrónica

trulheiro, com a inserção dos elementos adicionais recolhidos no terreno;
- Coligir os restantes dados e correlacionar a informação, de forma a consubstanciar a investigação conducente ao processo-crime (SIIOP).
- Incrementar a utilização de sistemas de informação geoespacial, de forma a obter padrões criminais; efetuar um *geoprofiling* e desenvolver modelos preditivos e preventivos de comportamento e de fenómenos socio-criminais, de forma a reduzir a criminalidade e a probabilidade de concretização de acidentes.

3.2 Reforçar a interoperabilidade e conetividade entre SI

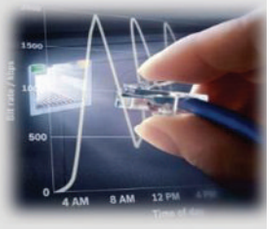
- Consolidar o Sistema Integrado de Informação Criminal (SIIC)[3] e privilegiar a partilha de informações via Plataforma de Intercâmbio de Informação Criminal (PIIC);
- Garantir a interoperabilidade com a 2.ª geração do Sistema de Informação Schengen (SIS II), de forma a possibilitar o acesso a dados biométricos; efetuar a ligação entre diferentes objetos (e.g. entre uma pessoa e um veículo) e possibilitar pesquisas diretas entre o SIIOP e o SIS II, assim como com os sistemas dos vários parceiros que contribuem para a segurança nacional e internacional[4];
- Incrementar a interoperabilidade e o automatismo, de forma a eliminar redundâncias na introdução de dados semelhantes, em sistemas de informação distintos;
- Implementar um serviço de *Helpdesk* transversal a todos os sistemas de informação da Guarda e assegurar serviços de apoio e suporte técnico às unidades apoiadas, através de plataforma colaborativa;
- Promover a integração entre a componente operacional e a de recursos internos, através do desenvolvimento de interfaces que garantam interação e interoperabilidade entre o SIIOP e os subsistemas integrantes do SIGRI, designadamente e como exemplos, entre serviços operacionais efetuados e remunerações, e na conexão entre a quilometragem das viaturas e as necessidades de manutenção;
- Integrar a ordem de serviço, mapa de férias e passaporte eletrónico, refletir a componente operacional diretamente nos abonos e associar a colocação de pessoal com a imediata disponibilidade para o serviço operacional, de forma automatizada e centralizada a todo o dispositivo da Guarda.

Acompanhar os desenvolvimentos técnicos externalizados

3.3 Privilegiar o recurso a novas tecnologias de informação

- Desenvolver um modelo de gabinete totalmente digital, assente na desmaterialização da informação, desde o Patrulheiro até ao mais elevado nível de decisão, garantindo a inexistência de documentos analógicos;
- Utilizar dispositivos de conversão e transcrição digital de voz para texto com elevados níveis de automatização, em prol da investigação criminal;
- Prover o Patrulheiro com equipamentos de tradução linguística digital, com entrada de voz analógica e saída de voz digital, para utilização com cidadãos estrangeiros e em comunidades de língua oficial não portuguesa;
- Utilizar equipamentos móveis digitais para recolha de prova, identificação de pessoas e disponibilização de forma resumida, das evidências recolhidas ao acusado ou ao seu representante legal, sendo os elementos digitais enviados para tribunal de forma totalmente eletrónica;
- Com os equipamentos móveis, digitalizar e capturar diretamente, a informação contida

Reforçar Interoperabilidade



[3] - Com especial enfoque no Art.º 3.º da Lei n.º 73/2009 de 12 de Agosto.
[4] - Relevando o Art.º 14.º da Lei n.º 74/2009 de 12 de Agosto.

nos documentos de identificação, confirmando a sua validade, cruzar esses dados com o registo automóvel e de embarcações, possibilitando a passagem imediata da contraordenação e da notificação para o respetivo *e-mail* do infrator;
- Implementar a gestão documental digital, definindo estrutura hierárquica de despacho, assinatura eletrónica e pontos únicos de entrada de correspondência em cada unidade;
- Preservar e catalogar os documentos através da sua digitalização e arquivo, de forma normalizada; Utilizar mecanismos de assinatura eletrónica, baseados no Cartão de Cidadão, prevendo a integração neste de dados profissionais;
- Certificar atributos profissionais, recorrendo ao Cartão de Cidadão;
- Garantir formação adequada e validação dos factos relevantes, recorrendo à plataforma de gestão do conhecimento disponibilizada *online* e com conteúdos específicos para a componente operacional;
- Implementar uma nova *intranet* da GNR, com melhores serviços de gestão documental e de conteúdos, mais colaborativa e mais alinhada com as diferentes necessidades e expetativas de informação dos seus utilizadores. O seu funcionamento, as dinâmicas de gestão de conteúdos e os diferentes *roles* dos seus colaboradores serão regulados através de um *governance plan*;
- Implementar um novo *site* oficial da GNR para ambiente *web*, numa versão móvel, do tipo multiplataforma e aplicação *Facebook*. Deverá ser mais moderno, seguro, usável, com áreas reservadas à comunicação social e deve conter conteúdos mais atualizados, definidos pelas diversas unidades, direções e serviços da GNR.
- Desenvolver uma rede social interna para interagir, difundir boas práticas, efetuar partilha colaborativa, troca de experiências e possibilitar serviços de apoio e suporte técnico, informais, entre os militares da Guarda;
- Implementar uma plataforma *online* para comunicação com o cidadão sobre as suas principais preocupações de segurança, incluindo furtos, crimes, atividades preventivas, suspeitas ou simples ocorrências, que possibilite a efetivação da queixa através de assinatura, recorrendo ao cartão de cidadão ou identificador biométrico e permita a inserção de fotografias, vídeos e outros dados digitais.
- Potenciar a utilização da plataforma de comunicações unificadas (integrando vídeo, VOIP, rede móvel, presença e *Instant Messaging*), de forma transversal à Guarda;
- Acompanhar os desenvolvimentos técnicos externalizados, garantindo transferência e aquisição de *know-how* e competências para a Guarda;
- Participar em grupos de trabalho e influenciar o Decisor Político, procurando maior interação entre os sistemas da Administração Pública (através de *web services*) e acesso de forma mais aberta e automatizada a dados externos com interesse para a Guarda.

3.4 Incrementar atuação no ciberespaço

- Estabelecer uma doutrina, implementar boas práticas e coligir ferramentas habilitantes à obtenção de Ciberinteligência, a partir de redes sociais e informação não estruturada *big data*;
- Estabelecer uma doutrina e incrementar a capacidade de Análise Forense Digital de todo o dispositivo, com especial ênfase em zonas de ação com maior densidade populacional e índice de criminalidade;
- Desenvolver *Plugins* Sociais Policiais e procurar os parceiros mais adequados para a sua difusão e implementação;

Helpdesk transversal aos sistemas de informação

Interoperabilidade SIIOP-SIGRI

Recolha digital de Prova

Rede Social da GNR

Plataforma online furtos e atividades suspeitas

Plataforma de comunicações unificadas

Cyberpatrol

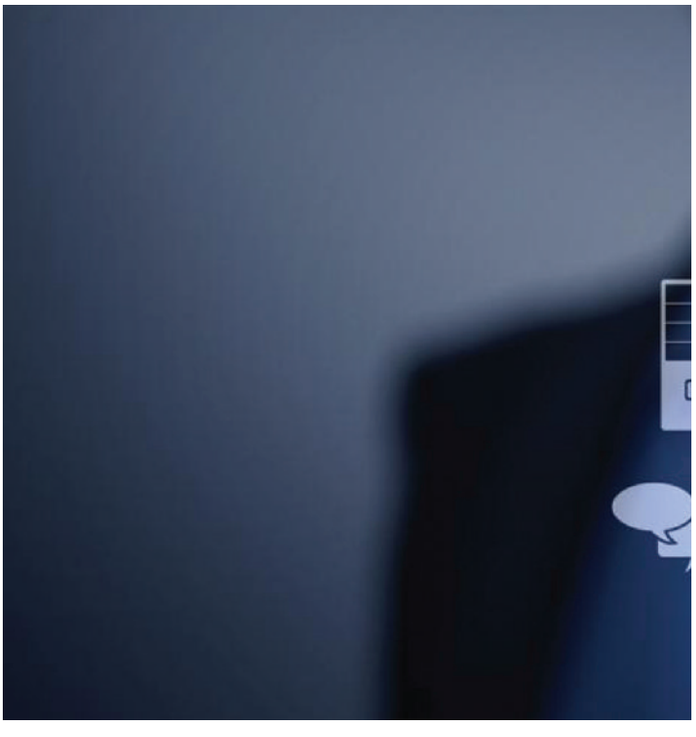
Análise Forense Digital

formação não estruturada *big data*;

- Estabelecer uma doutrina e incrementar a capacidade de Análise Forense Digital de todo o dispositivo, com especial ênfase em zonas de ação com maior densidade populacional e índice de criminalidade;
- Desenvolver *Plugins* Sociais Policiais e procurar os parceiros mais adequados para a sua difusão e implementação;
- Estabelecer e desenvolver modelo de "*Smart Security* GNR" com a finalidade de correlacionar eventos e dados obtidos no ciberespaço para efeitos preventivos e preditivos;
- Investigar e desenvolver ferramentas e metodologias que possibilitem as capacidades de *cyber patrol* e *cyber police*;
- Assegurar a exploração no ciberespaço, através de máquinas não associadas aos domínios GNR e RNSI.

3.5 Requalificar infraestruturas automóvel e tecnológica

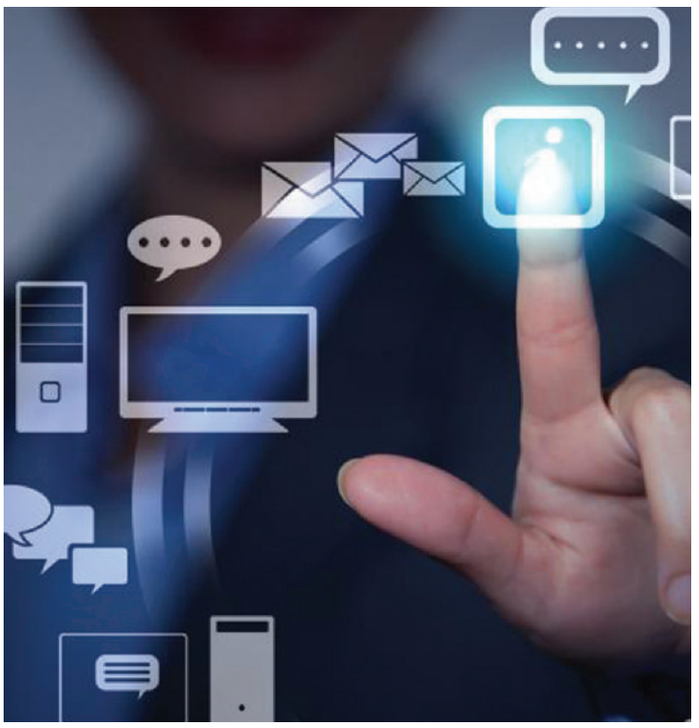
- Assegurar o acesso unificado (*single sign-on*) com o cartão de cidadão e/ou dados biométricos aos utilizadores dos sistemas internos, viaturas e infraestruturas da Guarda;
- Implementar Terminais de Dados Móveis (TDM) em viaturas e aos militares, com sistemas de aquisição de vídeo que, através de algoritmos de processamento automático de imagem e outros sensores possibilitem, de forma automatizada, o corelacionamento e integração de dados, a fim de obter a identificação de veículos e pessoas, recorrendo em Tempo Real a bases de dados e a redes sociais para precaver e proteger o Patrulheiro, tentando antecipar onde e quando o crime poderá acontecer;
- Recolha de som, imagem e vídeo pelos patrulheiros, através da utilização de equipamentos não obtrusivos, em que os *feeds* de informação serão transmitidos em formatos normalizados, a fim de poderem ser utilizados por outras FSS;
- Adaptar as capacidades das SSit de forma a funcionarem como Centros de Fusão, em tempo real, recolhendo os dados oriundos do patrulheiro e gerando inteligência após corroboração com outros temas, bem como efetuar a atribuição de missões ou ealocação dos elementos no terreno;
- Colocar TDMs com reconhecimento automático de matrículas a equipar as viaturas da Guarda, integradas com a rede estabelecida de sinais de trânsito luminosos, câmaras de vídeo na rede viária e outros sensores;
- Atribuir uma viatura para cada posto com capacidade de tração às quatro rodas, com um meio eletrónico (equipada com sistema GPS com visualização de cartografia militar) que permita navegar até qualquer ocorrência;
- Implementar a tecnologia RFID para os artigos, equipamentos e material, cujo posicionamento e controlo de acessos seja



considerado um fator crítico;
- Disponibilizar *online* manuais técnicos de viaturas e embarcações possibilitando a inserção de boletim de serviço digital da viatura pelas unidades e atores envolvidos;
- Garantir uma adequada catalogação e contabilização física do imobilizado das unidades, disponibilizando tecnologia de impressão e leitura óptica, de forma a garantir a completude dos dados do GeRFiP.
- Implementar a tecnologia RFID para os artigos cujo posicionamento e controlo de acessos seja considerado um fator crítico.

4 - CONCLUSÕES

O trabalho desenvolvido no âmbito do Grupo de Trabalho para as Tecnologias e Sistemas de Informação tem tido como objetivo primordial, a prossecução dos Objetivos Estratégicos e a operacionalização da Visão, segundo as Linhas de Orientação Estratégica definidas no documento "ESTRATÉGIA DA GUARDA 2020 - Uma Estratégia de Futuro", com a centralização de esforços no:



- Apoio ao militar no terreno, procurando garantir maior segurança no desempenho das funções e desburocratizar e desmaterializar processos;
- Racionalizar sistemas de informação e garantir a sua interoperabilidade;
- Incrementar a qualidade do processo de decisão hierárquico, através da melhoria do comando e controlo de alto nível, garantindo transversalidade estrutural e especificidade de cada área.

Outra das vertentes evolutivas tem consistido no refinamento do modelo de governação das TSI na Guarda, designadamente, adaptando a estrutura de autoridade e responsabilidade para coordenação e execução dos processos, o qual é conducente a uma implementação mais efetiva de políticas, normativos e garante à racionalização dos recursos existentes, assegurando o alinhamento permanente das Tecnologias e Sistemas de Informação, com a estratégia de negócio da Guarda e garantindo a sua sustentabilidade na perspetiva de longo prazo.

Os objetivos de médio prazo consistem em colocar a Guarda na vanguarda digital das Forças e Serviços de Segurança nacionais e, paralelamente, em áreas específicas, acompanhar as nossas congéneres de referência internacional.

Como a visão do papel continua a ser desempenhado pelo GTTSI, considera-se:

"Liderar a Guarda Nacional Republicana no seu futuro tecnológico, assegurando flexibilidade e adaptabilidade das tecnologias e sistemas de informação, de forma a garantir o apoio adequado às necessidades operacionais e de gestão."

Plataforma online furtos e atividades suspeitas

Plataforma de comunicações unificadas

Cyberpatrol

Análise Forense Digital

A interoperabilidade dos Sistemas de Informação como fator de sucesso

Sistemas de Informação

Um Sistema de Informação (SI) de uma organização é composto pelos recursos humanos, pela tecnologia e pelos processos de trabalho da organização, tendo em vista o armazenamento, o processamento, a distribuição e a transmissão de informação útil e oportuna, de forma a satisfazer as necessidades de informação e potenciar soluções e a satisfação de novos desafios para a organização.

Os SI assentam, essencialmente, nas pessoas e nos processos de trabalho, agilizados por um conjunto de componentes interrelacionados que permitem reunir, procurar, processar, armazenar e distribuir informação, com o objetivo de suportar o processo de tomada de decisão e o controlo dos recursos de uma organização nos vários níveis de gestão.

No respeitante aos níveis de gestão, os SI podem ser classificados em Sistemas de Informação de Nível Operacional, de Nível Gestão e de Nível Estratégico:

- Os de Nível Operacional processam e registam as transações diárias de rotina, e têm como base um elevado conjunto de dados tabelados.
- Os de Nível de Gestão monitorizam e controlam o processo de tomada de decisão, fornecem relatórios periódicos e fazem a análise da evolução das tendências no espaço e no tempo, em diferentes referenciais (geográfico, orgânico, recursos humanos, recursos materiais, etc.).
- Os de Nível Estratégico controlam os objetivos de longo prazo e são a base para definição de políticas e orientações estratégicas, tendo em conta tanto o ambiente interno, como o ambiente externo da organização.

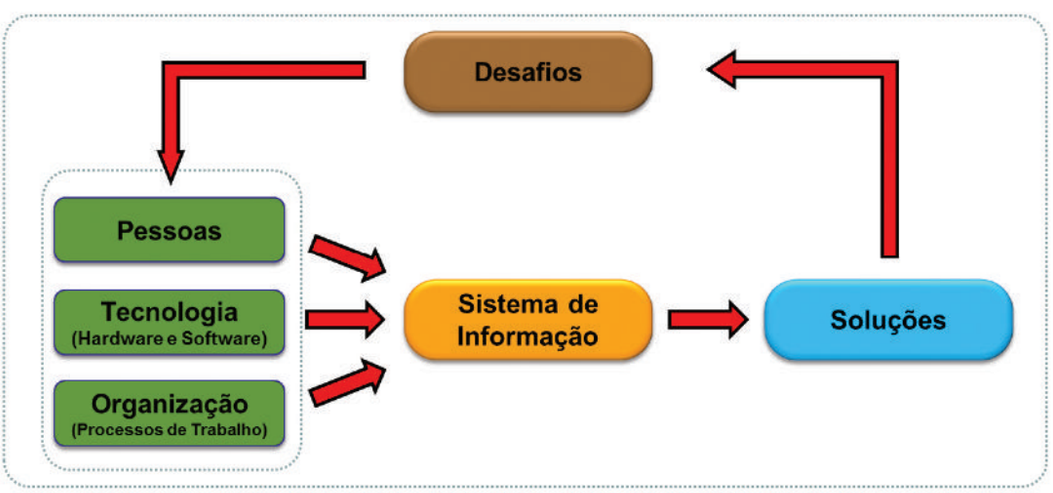


Figura 1 – Diagrama simplificado de um Sistema de Informação

Figura 2 – Tipologia dos Sistemas de Informação

Todas as áreas funcionais de uma organização (por exemplo recursos humanos, manufatura e produção, contabilidade, formação, financeira, vendas e *marketing*) podem ser apoiadas por sistemas de informação dos tipos de nível operacional, de gestão e estratégico. Desde que assegurada a correta interoperabilidade entre os vários sistemas de informação, é possível, a partir dos dados, obter informação e conhecimento, potenciando a sabedoria e a antecipação de situações futuras, conforme indicado no modelo DIKW (*Data, Information, Knowledge and Wisdom*) espelhado na figura 3.

Os Sistemas de Informação da Componente Operacional da GNR

No Comando Operacional da GNR, o apoio ao processo de tomada de decisão é suportado por vários Sistemas de Informação dos quais se destacam:

- O SG2S (Sistema de Gestão de Salas de Situação) que regista todas as ocorrências e realiza o despacho de meios.
- O SGO-SITREP (Sistema de Gestão Operacional/ /SITREP) que regista todas as ocorrências criminais, detenções, diligências, resultados de operações, etc.

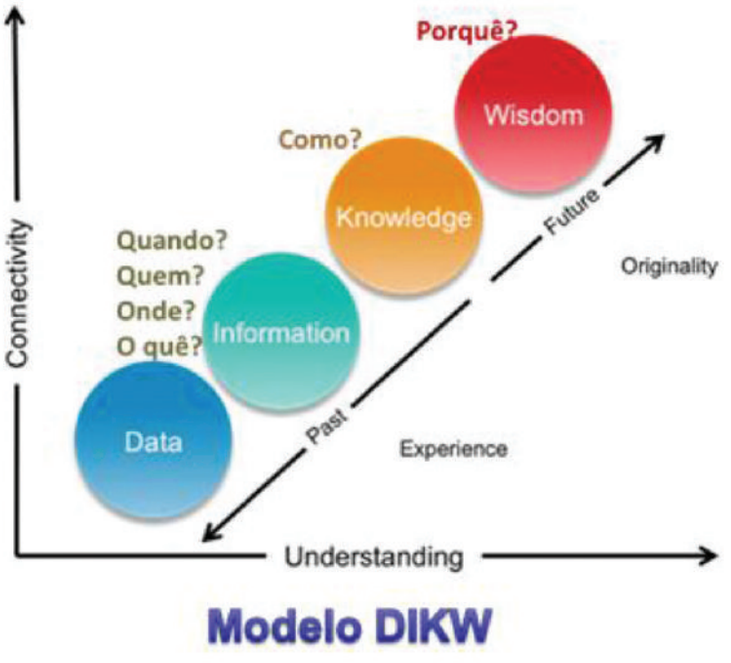


Figura 3 – Modelo DIKW (*Data, Information, Knowledge and Wisdom*)

- O SGR (Sistema de Gestão Rodoviária) que regista todas as ocorrências de sinistralidade e fiscalização rodoviária, bem como a informação relativa às vias interditas, sendo possível produzir o BEAV (Boletim Estatístico de Acidentes de Viação).
- O SGS (Sistema de Gestão SEPNA) que regista todas as ocorrências ambientais e de proteção da natureza.
- O *E-Briefing* que é uma ferramenta de nível de gestão que se liga ao SGR e ao SGO-SITREP, para permitir a apresentação de resumos e estatísticas sobre a sinistralidade e a criminalidade diárias, bem como a georreferenciação das incidências mais relevantes.
- O GNR*Mobile* que permite implementar o conceito de mobilidade da GNR (em tecnologia *Android*), onde cada militar poderá aceder a um conjunto de informação sobre quais os procedimentos a tomar, face a determinada situação operacional, bem como reportar uma necessidade de apoio e, em certos casos operacionais, emitir RELIM's (Relatórios Imediatos) de forma abreviada.
- O SIIOP (Sistema Integrado de Informações Operacionais de Policia) é o principal sistema de informação operacional, utilizado para armazenar dados relativos a toda a atividade operacional, potenciando a uniformização de processos de trabalho da GNR, a unicidade da informação, o registo de informação objetiva e especulativa, a elaboração de relatórios periódicos, a partilha de informação tanto internamente, como com entidades externas (PSP, PJ, SEF, Policia Marítima, Ministério Público, ANSR) e a análise de grandes volumes de dados, de forma a apoiar o processo de tomada de decisão.
- O SIG-GNR (Sistema de Informação Geográfica da GNR) que através da utilização centralizada de mapas digitais, faz a identificação de zonas de competência das unidades da GNR, divisão administrativa, registo de ocorrências, pontos importantes e outra informação considerada de interesse para a Guarda.
- O SIG-SIRESP (Sistema de Informação Geográfica dos meios SIRESP) que implementa o COP (*Common Operational Picture*) da GNR, através da visualização dos meios no terreno.

De forma a garantir a disponibilidade e a unicidade da informação, existe a necessidade de interoperar os sistemas acima referidos, havendo a necessidade de desenvolver trabalhos para a informação fluir para o SIIOP.

Desta forma, o modelo DIKW da atividade operacional da GNR poderá, no futuro, ser construído com base na interoperabilidade dos sistemas SG2S, SGO-SITREP, SGR e SGR com o SIIOP e com o SIG-GNR, para permitir análises espaciais e tem-

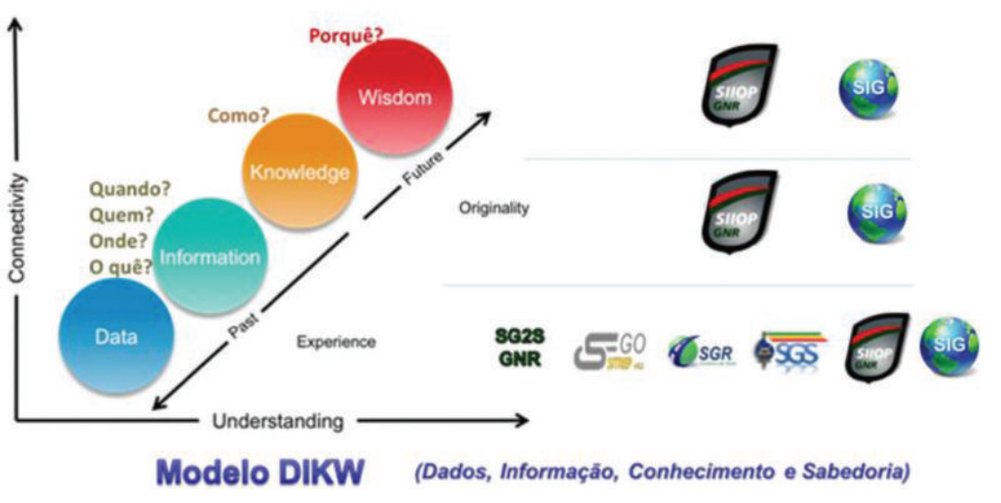


Figura 4 – Modelo DIKW da atividade operacional da GNR

porais com capacidade de implementação de modelos preventivos e preditivos de ocorrências criminais e de sinistralidade.

Os Sistemas de Informação Estratégicos da GNR

Tendo por base os Sistemas de Informação respeitantes à atividade realizada no Comando Operacional, identificou-se o SIIOP e o SIG-GNR como sendo Estratégicos, que devem contribuir para o projeto de interoperabilidade da GNR.

Na área de atividade dos Comandos da Administração dos Recursos Internos, da Doutrina e Formação e do Comando da Guarda, identificou-se o SIGRI (Sistema Integrado de Gestão de Recursos Internos) que se constitui numa plataforma modular que agrega os Sistemas de Informação de Gestão de Pessoal (SIGPES), Vencimentos (SIGVC), Apoio à Saúde (SIGSAD), Finanças e Orçamento (SIGFO), Formação (SIGFORM), o Plano de Atividades e o Plano Estratégico, a partir de um repositório de dados comuns. O SIGRI também permite a interoperabilidade com o Portal Social que se torna uma importante ferramenta para a GNR comunicar com os seus militares.

Ao considerar a restante atividade da GNR, pode-se verificar que, devido às diferentes missões e aos processos implementados nas diferentes unidades, à dispersão territorial, ao elevado volume de informação a tratar e ao excessivo uso do papel, a GNR nunca teve a possibilidade de uniformizar e adotar um sistema único de gestão documental, existindo a necessidade de implementar uma capacidade integradora para uniformizar os processos documentais, o arquivo e o tráfego de documentação militar, devendo este sistema ser considerado estratégico, por contribuir para a implementação da uniformização dos processos de trabalho da Guarda.

Face ao acima referido, considera-se que os principais sistemas a contemplar para um projeto de interoperabilidade global, ao nível de toda a atividade da GNR são o **SIIOP**, o **SIGRI**, o **SIG** e a **Gestão Documental** única (a implementar logo que possível).

Projeto de interoperabilidade dos principais sistemas de informação na GNR

Torna-se muito importante implementar um conceito de interoperabilidade entre os principais sistemas de informação da GNR, tendo sido criado, no âmbito da Estratégia 2020, o *Projeto de interoperabilidade dos principais sistemas de informação da GNR*.

Uma vez considerados os quatro sistemas de informação estratégicos acima referidos, torna-se necessário fazer um levantamento exaustivo dos processos de trabalho que requeiram dados destes diferentes sistemas, para garantir o correto fluxo de dados e a interoperabilidade.

É importante referir que, a tecnologia não se constitui como elemento principal do projeto, devendo ser dado realce às pessoas e aos processos de trabalho da GNR, razão pela qual e devido ao elevado volume de informação, à diversidade de matérias funcionais e às múltiplas especificidades, é necessário que o levantamento e a priorização dos processos de trabalho funcionais seja levada a cabo pelos responsáveis de cada área de atividade, tendo por base o impacto na atividade da GNR, a sua interação com o cidadão, com as empresas e com o próprio Estado.

Para cada processo de trabalho funcional com necessidades de interoperabilidade deverá ser identificado:

- Que dados são importantes (O quê)?
- Qual a sua função (Para quê)?
- Os dados estão em rede (Onde)?
- Que entidades devem aceder a esses dados (Quem)?
- Qual o período de utilização/disponibilização (Quando)?
- Qual a motivação (Porquê)?

Após o levantamento dos dados necessários aos diversos processos, é necessário planear a sua integração num novo sistema ou planear a sua interoperabilidade direta com entidades internas ou externas (podendo o sitio da GNR vir a ser considerado um SI que contribui como charneira para interoperabilidade externa da GNR).

Em termos tecnológicos, deverão ser equacionados trabalhos de engenharia (com possibilidade de recurso a *outsourcing*) para o desenho dos processos a integrar/interoperar, sua implementação e operacionalização, através da construção de um *Enterprise Service Bus* com conetores às aplicações atualmente em funcionamento.

Este projeto de interoperabilidade assume uma importância vital para a Guarda, exigindo empenho de meios e esforço de coordenação, não se apresentando como uma rápida solução de problemas, mas antes um desafio a vencer que colocará uma Guarda detentora de Sistemas de Informação inovadores, contribuindo para melhores práticas e para uma melhoria do serviço prestado ao cidadão.

Tenente-Coronel JOÃO NUNES

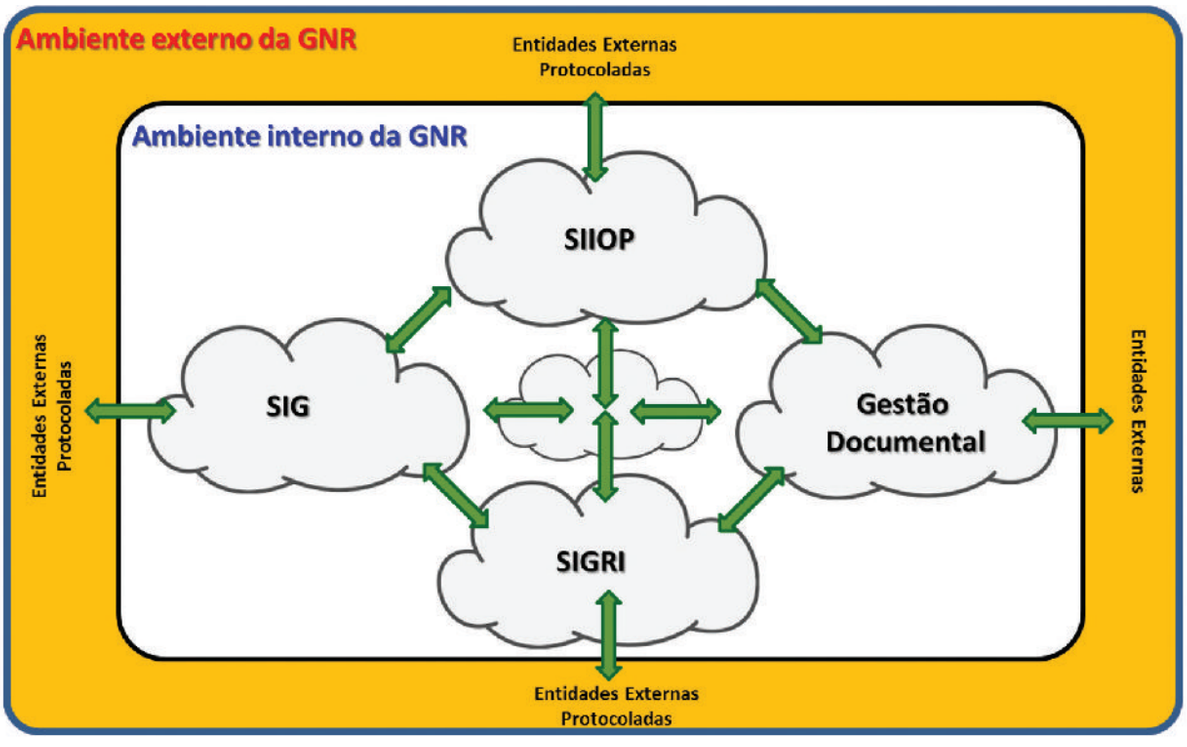


Figura 5 – Projeto de interoperabilidade dos Sistemas de Informação da GNR

Referências:
1 - ANDREW S. TANENBAUM, "Modern Operating Systems", Pearson Education International, 2009.
2 - KELLY RAINER, BRAD PRINCE & CASEY CEGIELSKI, "Introduction to Information Systems – Supporting and Transforming Business", 5th Ed, Wiley, 2013.
3 - KENNETH LAUDON & JANE LAUDON, Management Information System, 12th Ed, Pearson Education International, 2011

Inovação Tecnológica no Ciberpoliciamento "Police Social Plugins"

" A melhor maneira de predizer o futuro é fazê-lo
(...) Todas as inovações eficazes
são surpreendemente simples "

Peter Drucker

O Valor da Inovação

Atualmente, o mundo encontra-se ao nível social, político e económico, num imparável processo de mudança sem paralelo, na história da nossa civilização. Os efeitos da globalização e a existência, à escala planetária, de um estado de permanente interconetividade, aceleram e reforçam este processo de mudança, o qual é tremendamente influenciado pela força motriz da Inovação Tecnológica que desafia a Sociedade a projetar e a implementar, de forma incessante, novos "produtos", "serviços" ou "paradigmas", em todas as áreas da atividade humana.

A presença ou a ausência de soluções tecnológicas e toda a "logística informacional" associada à vida das pessoas, das organizações ou das instituições, resultantes da síntese de um determinado processo de "Inovação" pode torná-las mais adaptáveis, competitivas e proficientes, de modo a satisfazer as expetativas e necessidades dos seus beneficiários.

Atualmente, o serviço policial compreende um largo espetro de atuação na área da segurança e ordem pública, regulação e fiscalização rodoviária, no plano fiscal e aduaneiro, apoio e socorro, controlo costeiro e na área da cibersegurança. Nestes domínios, a atuação das Forças e Serviços de Segurança (FSS) caracteriza-se pela multiplicidade de respostas que devem estar capacitadas a dar e pela heterogeneidade das intervenções policiais, que vão desde a simples facilitação de informações ao cidadão até às funções que requerem elevada competência técnica, como as atividades no âmbito da investigação criminal ou a recolha e análise de

Figura 1 – Arquiteturas fundamentais de um Sistema de Informação

dados para produção de "inteligência policial". Estes tipos de *expertise* deverão ser suportados em **Sistemas de Informação Policiais bem projetados e dimensionados, o que só é possível, através de um processo de conjugação perfeita entre a chamada "Engenharia Organizacional" – Pessoas, Processos de Trabalho, Organização, e a "Engenharia Tecnológica"- *Hardware* e *Software***, associada a uma adequada "*IT Governance* Policial".

Nesta contextura, a recente **"Agenda Europeia de Segurança[1] de 2015**" identifica **três prioridades de prevenção e de repressão criminal que os Estados Membros da UE devem perspetivar nos próximos cinco anos: o combate ao Crime Organizado, o Terrorismo e o Cibercrime**. Os atores deste tipo de criminalidade utilizam cada vez mais "Tecnologias de Informação e de Comunicação (TIC)" disruptivas (inovadoras), por forma a tornar a gestão do seus "negócios criminais" altamente competitiva, lucrativa, sofisticada e cada vez mais autómata. As Forças de Segurança só conseguirão travar os efeitos destas realidades criminais, se criarem estratégias genéticas, estruturais e operacionais que permitam acompanhar e compreender melhor as variáveis da inovação tecnológica que são utilizados pelos novos atores criminais.

Assim sendo, as estratégias estruturais e operacionais a serem adotadas pelas Forças de Segurança deverão convergir no uso intensivo de **dispositivos e sistemas de informação[2](SI) especialmente orientados para a recolha e análise holística de informação**. Estes SI deverão permitir que o processo de apoio à tomada de decisão se possa processar em diferentes cenários criminais, especialmente aqueles em que existe a cada vez maior "constante da incerteza". A denotar que a eficiente gestão da incerteza ou da imprevisibilidade criminal só é possível quando qualquer Força de Segurança tem, por um lado, a capacidade inicial e real de recolher "Dados" com qualidade (Completos, Fiáveis, Coerentes, Oportunos, Acessíveis), visando transformá-los em "Informação", e, posteriormente, em "Conhecimento" preditivo. Isso

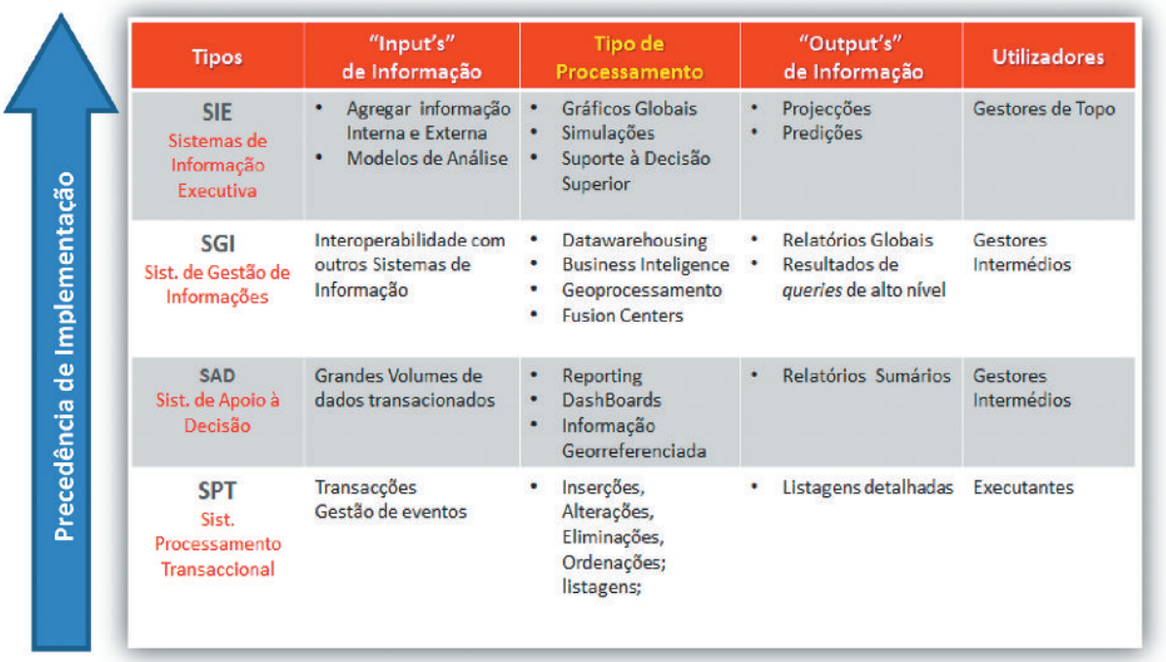


Figura 2 – Matriz de Sistemas de Informação vs Cenários de Utilização

[1] The European Agenda on Security, Strasbourg, European Comission, 28.4.2015 COM(2015) 185 final

[2] Sistemas do tipo SOA (Service Oriented Architecture)

só é possível com SI que sejam projetados de forma logica e sistémica, a partir de diferentes "cenários de utilização" agregados a distintas tipologias de utilizadores. Reforça-se, que a projeção desses SI deverá realizar-se através da conjugação perfeita entre a (Re)engenharia Organizacional e a Engenharia Tecnológica, num processo dinâmico de inovação, em que o investimento no capital humano alinhado com "*IT Governance*" é condição *sine qua non* para permitir a eficácia policial nas conjeturas criminais atuais.

O Ciberespaço, as Redes Sociais e as Atividades Delituosas

Presentemente, o ciberespaço é a convergência entre o meio físico e o virtual. A partir dele processam-se novas dinâmicas sociais, económicas, políticas e culturais. Todas as atividades humanas estão presentes neste tremendo e ininterrupto espaço de conetividade. Nesta dimensão, o grau de penetração das redes sociais na sociedade é enorme, como comprovam os dados estatísticos de 2014, que são veiculados pela agência internacional "*whe are social*":

Depreende-se daqui, que as redes sociais constituem um fenómeno sem precedentes de interação *online*, de comunicação e de socialização em larga escala, sendo gerados a partir delas, diferentes tipos e formatos de conteúdos (texto, áudio, vídeo, imagens, etc), constituindo um "e-organismo" em constante expansão, onde são geradas incessantes dinâmicas de "oportunidade" que potenciam por um lado, a evolução da sociedade, mas também de forma espontânea, atividades delituosas massivas. Em suma, todas as atividades ilícitas levadas a cabo no "mundo físico" convergem e encontram-se cada vez mais intimamente ligadas às Redes Sociais, sendo que as mais prevalentes são:

- Aumento das atividades dos predadores e dos assédios sexuais;
- A violação de dados pessoais com intenções maliciosas cometida através da Engenharia Social;
- Ações de "*Phishing*" (ex: acesso a dados bancários, números de telefone, endereços postais, dados de nascimento, etc);
- A proliferação de *software* malicioso;
- O aumento das fraudes (ex: vendas de vistos, ofertas de emprego fictícios, venda de bens que não existem, transferência de dinheiro através de contas *online* fraudulentas, etc);
- Incitação de distúrbios de Ordem Pública.
- Fins propagandísticos, de mobilização e para o recrutamento de militantes, obtenção de fundos e de financiamento de atividades terroristas.

Figura 3 – Estatísticas de Utilização da Internet e das Redes Sociais de 2014

A realçar-se que a superfície de projeção de um ato ciberdelinquente ou criminal é muito elevado nas redes sociais. Isto é potenciado principalmente, pelo alto grau de presença que a *internet* tem em todas as atividades da sociedade; por causa da falta de informação que os cidadãos têm relativamente às ameaças que existem nesta rede; porque existem "dinâmicas de oportunidade e de aprendizagem" do delito maiores do que aquelas que existem no "mundo real"; pelo anonimato que os seus autores (pessoas, organizações ou Estados) usufruem neste meio e pelos baixos índices de censurabilidade e de "controlos" (princípios, valores éticos, normas) existentes no ciberespaço;

Ciberpoliciamento através de Engenhos Sociais "*Safety Social Plugins*"

O desenvolvimento de novas capacidades de ciberpoliciamento no contexto das redes sociais, fazendo uso de tecnologias sociais, pode representar uma oportunidade e um veículo decisivo para as forças de segurança serem capazes de interagir diretamente com o cidadão, com as organizações ou com as instituições, podendo assim permitir:

- Conduzir programas de Ciberprevenção e de "*Cyber awareness*[3]";
- Recolher informação de várias fontes advenientes das Redes Sociais;
- Proceder a ações de Investigação Criminal;
- Ações de Prevenção do Crime;
- Manter a Ordem Pública;
- Prestar apoio a Vítimas e Proteção Civil

Mas para isso ser possível, é fundamental compreender e dominar os paradigmas e a arquitetura tecnológica em que as diversas redes sociais estão estruturadas. A título de exemplo, a bem conhecida rede social "*Facebook*" utiliza os chamados "*plugins* sociais" ou engenhos sociais para ligar, de forma viral, pessoas, dispositivos, plataformas ou objetos no ciberespaço. Os *plugins* mais conhecidos são o botão *Like*, *Activity Feed*, *Facepile*, *Comment*, *Share button*, *Recommendations Button*, *Send Button*.

Cada um destes engenhos tem funções diferentes e são complementares entre si, podendo ser subscritos pelos utilizadores e embebidos em qualquer dispositivo, páginas *web* ou em diferentes plataformas que existam no Ciberespaço.

Figura 4 – Plugins Sociais do *Facebook*

O objetivo principal dos "*plugins* sociais" é, de forma ininterrupta, veicular e potenciar experiências e interações sociais entre pessoas, comunidades, organizações, etc. Por outro lado, eles constituem o engenho fundamental para o *Facebook* poder recolher de forma exponencial, dados dos seus utilizadores, conduzir o chamado "*marketing* social" e levar a cabo os seus diversos processos de negócio.

No escopo do anteriormente referido, a GNR concetualizou um novo conceito no plano da ciberprevenção e ciberpoliciamento. O conceito foi apresentado durante o ano de 2015, em diversos

[3] Cultura de Cibersegurança e Consciência das Ciberameaças

fóruns internacionais, sob a designação de "*Police Social Plugins*", nomeadamente, na "Reunião da Comissão Novas Tecnologias e Logística da FIEP" em França, bem como num seminário organizado pela *Gendarmerie Nationale* Argelina, no âmbito da "Iniciativa 5+5" que se subordinou ao tema "A Cibercriminalidade: As Redes Sociais e a Segurança Pública".

O conceito consiste, essencialmente, em projetar e desenvolver "*plugins* sociais" orientados ao policiamento comunitário no ciberespaço, utilizando tecnologicamente as bibliotecas de funções (API's) que cada uma das redes sociais atuais já disponibiliza. Estes engenhos permitirão potenciar, por contágio social, diferentes dinâmicas de ciberprevenção em rede e, ao mesmo tempo, a produção de "*Cyber Intelligence*", visando deste modo, garantir um "Conhecimento Situacional" mais robusto acerca de atividades delituosas no Ciberespaço.

Visa-se, pois, desenvolver um conjunto de "*plugins* sociais" com serviços diferenciados, no sentido de potenciar a segurança participativa e comunitária entre os diversos atores (cidadãos, empresas, academias, órgãos do Estado, etc) que interagem no ciberespaço, tendo como especial orientação os preceituados enunciados pela própria "Estratégia Nacional de Segurança do Ciberespaço" e a "Estratégia de Cibersegurança da União Europeia".

Neste contexto, prevê-se que a GNR irá, em parceria com a empresa portuguesa "*Whale*", a Universidade Nova de Lisboa, IMS e a Universidade da Beira Interior, participar num projeto nacional designado por "Engenhos Sociais Orientados à Segurança – ESOS", o qual se prevê que possa vir a materializar este novo paradigma que pode vir a constituir uma inovação no policiamento do Ciberespaço.

A GNR, através da conceção deste tipo de soluções

Figura 5 – Exemplos de possíveis *Police Social Plugins*

inovadoras pretende, ao nível da Cibersegurança, ser cada vez mais uma Força de Segurança distinta e moderna, preparada para fazer face aos novos desafios criminais que se colocam ao nível do ciberespaço, de forma a elevar a Consciência Coletiva para os comportamentos de risco relacionados com o simples ciberdelito, à cibercriminalidade ou até mesmo a atividades subversivas no ciberespaço, em que se inclui o (ciber)- terrorismo.

Em última análise, a GNR, numa dinâmica de segurança comunitária e participativa, pretende contribuir para um Ciberespaço mais Desenvolvido, Seguro e Democrático, reforçando assim, a chamada "Cidadania Digital", numa escala "sem fronteiras".

Tenente-Coronel PAULO SANTOS

Bibliografia

LAUDON, K., 2012, Management Information Systems (12th Edition), Prentice Hall
Resolução do Conselho de Ministros n.º 36/2015, "Estratégia Nacional de Segurança do Ciberespaço"
JOIN (2013) 1 final, 7.2.2013, "Cybersecurity Strategy of the European Union, European Comission"
COM (2015) 185 final, 28.4.2015, "The European Agenda on Security, Strasbourg, European Comission"
https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015
http://wearesocial.net/

SIG-Modelos de análise preventiva e preditiva de fenómenos criminais (Crime Mapping e Geoprofiling)

O Sistema de Informação Geográfica é um sistema computacional para a manipulação, consulta e análise de informação, referenciada a um dado espaço geográfico. Potencia os sistemas de informação convencionais, analisando e correlacionado a informação digital corrente com a sua localização espacial, dando uma visão mais ubíqua sobre os dados. Permite a obtenção de informação com base em atributos alfanuméricos e a dedução de relações de proximidade, vizinhança, sobreposição e o envolvimento entre dados.

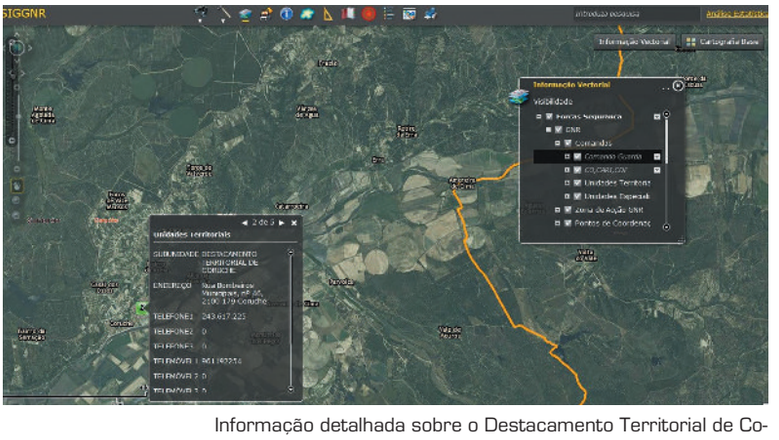
Estes Sistemas de Informação representam um papel preponderante em questões de localização, ao permitir inquirir as características de um lugar em concreto.

Em termos de avaliação de contexto para a área de intervenção, nomeadamente, as características demográficas, económicas, sociais e físicas, este sistema de informação é crucial.

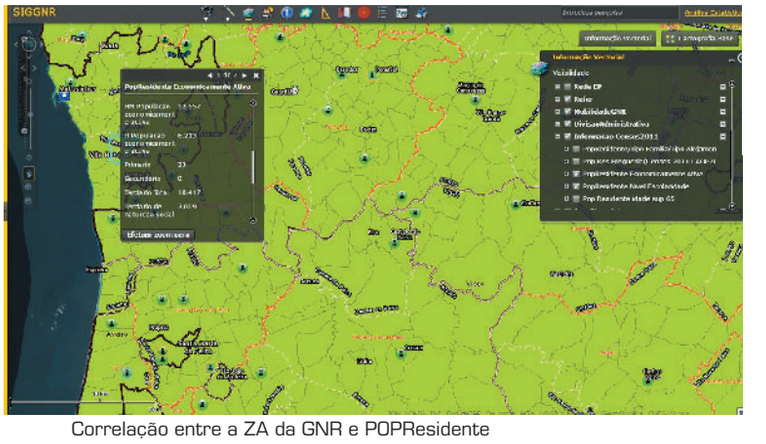
Este sistema é decisivo para simular cenários de ocorrências, avaliar os impactos das intervenções, efectuar mapas de ocorrências, produzir mapas de riscos "pontos Negros" (real, potencial e resultante da percepção de risco pelos habitantes).

Em assuntos de comparação entre situações temporais ou espaciais distintas de alguma característica, o SIG é fulcral.

Este sistema de informação é imprescindível no cálculo de percursos óptimos entre dois ou mais pontos de comprimento ou não, de condições impostas

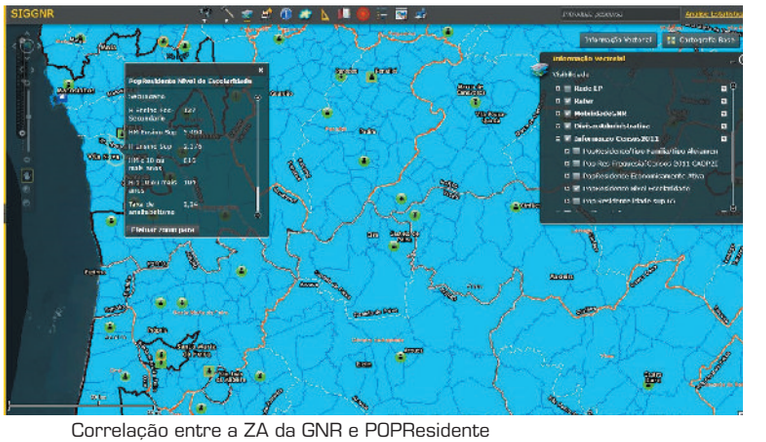


Informação detalhada sobre o Destacamento Territorial de Coruche

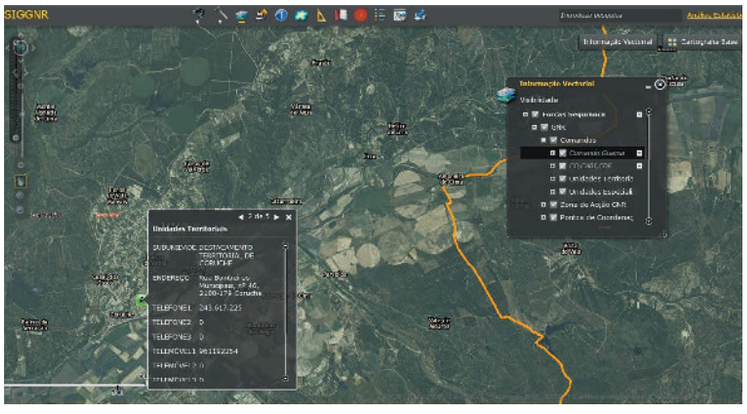


Correlação entre a ZA da GNR e POPResidente da Freguesia economicamente ativa

Informação detalhada sobre a Zona de ação do Posto Territorial de Estremoz

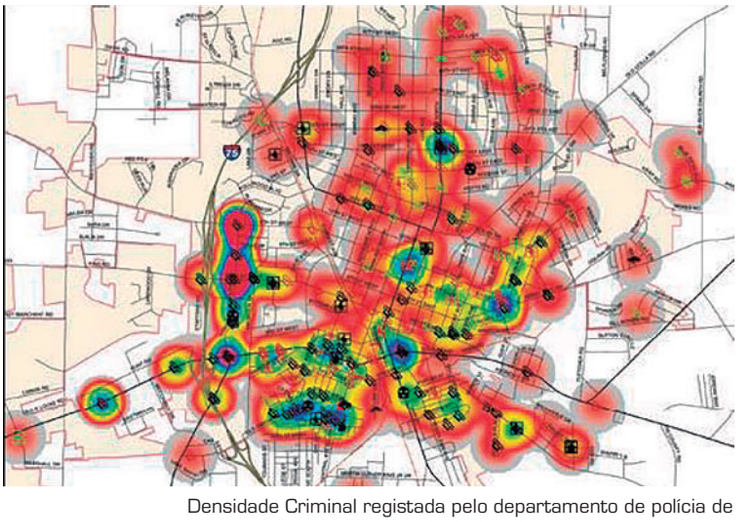


Correlação entre a ZA da GNR e POPResidente da Freguesia Nível de Escolaridade

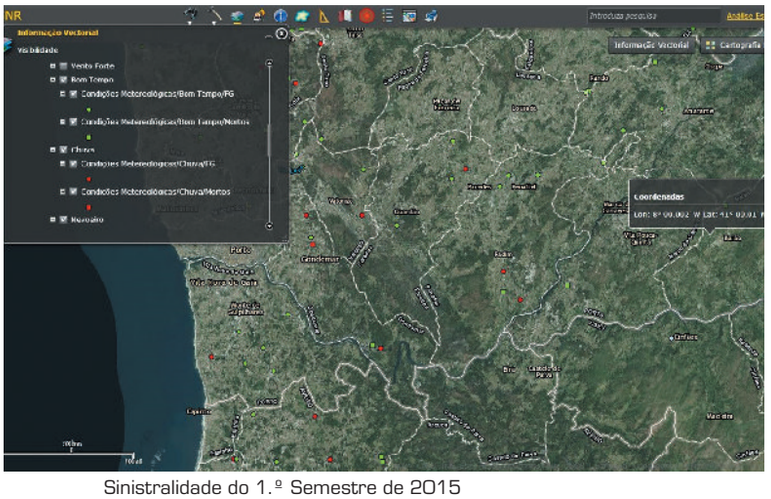


HotSop da Sinistralidade do 1.º Semestre de 2015
de Portugal Continental

Sinistralidade do 1.º Semestre de 2015
Condições Metrológicas/Bom Tempo



Densidade Criminal registada pelo departamento de polícia de
LIncoln, Nebraska



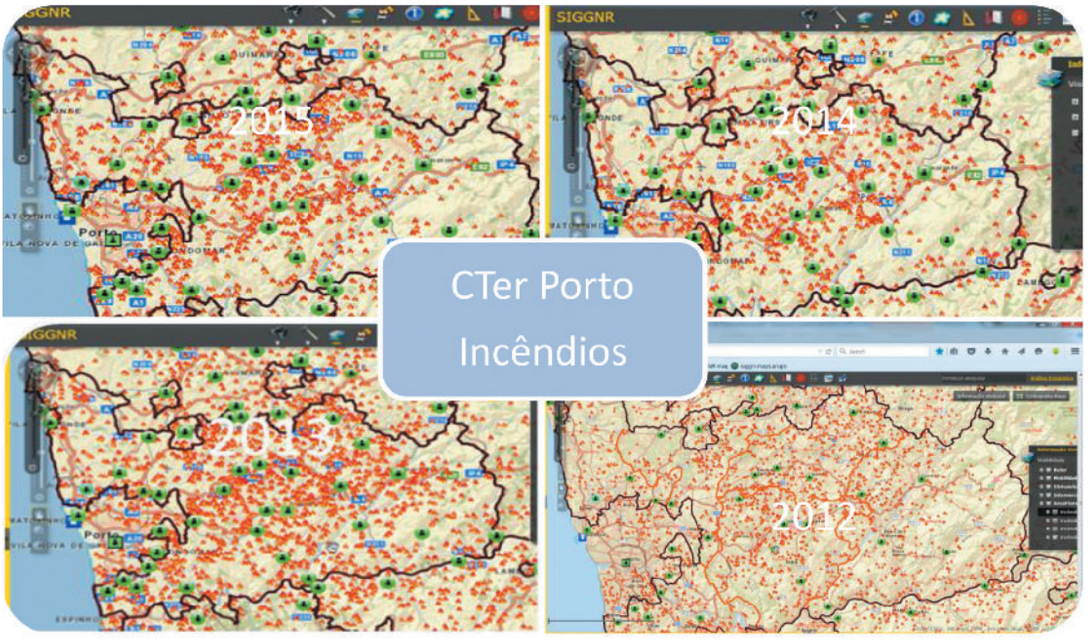
Sinistralidade do 1.º Semestre de 2015
Condições Metrológicas

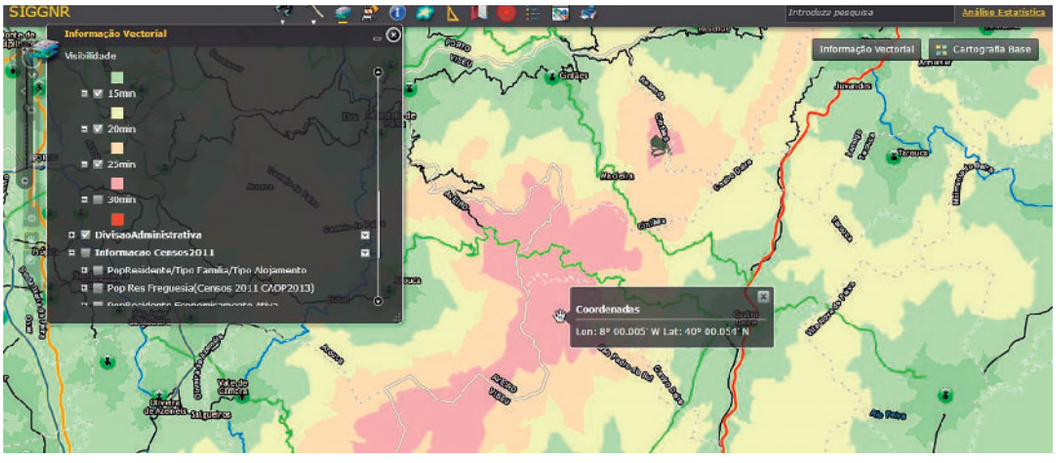
aos objectos, de geração de modelos explicativos, a partir do comportamento observado de fenómenos espaciais de gestão de recursos, uma vez que possibilita uma percepção global do espaço, dada a quantidade de informação associada, a sua organização e a facilidade de consulta de dados.

O Sistema de Informação geográfica é essencial para determinar o perfil geográfico. Este baseia-se no facto de os criminosos seleccionarem as suas vítimas e perpetrarem os seus crimes perto da sua área de residência. No caso dos predadores sexuais, foram realizados inúmeros estudos e ficou provado que existe uma área de conforto para estes cometerem os seus crimes, com um sentimento de segurança. Consequentemente, actos criminosos seguem uma função de distância decrescente, de modo a que, quanto mais longe o espaço regular de uma actividade delinquente é, menor a probabilidade de que a pessoa se vá envolver numa actividade criminosa predatória. No entanto, há também uma zona tampão onde um infractor vai evitar cometer crimes. Esta localiza-se muito perto da sua casa, uma vez que existe a possibilidade de ser identificado por um vizinho.

Outro factor chave no perfil geográfico assenta no facto do agressor e da vítima se cruzarem no tempo e no espaço antes do crime acontecer ou seja, possuírem rotinas em comum.

Os crimes em série são os mais fáceis de desenvolver perfis geográficos, uma vez que cada crime contém novas informações espaciais e fornece dados adicionais, incluindo o facto de que a área geográfica de criminalidade tende a aumentar com o aumento de conforto e confiança.





Rede viária e Isócronas a 5, 10, 15, 20 25 e 30m que permitem decidir qual a melhor unidade a responder a determinada ocorrência

O Centro de Informação Terrorista do Arizona usa SIG para protecção e avaliação de Infra-estruturas criticas

geográfica de criminalidade tende a aumentar com o aumento de conforto e confiança.

O Sistema de Informação Geográfica existente na GNR encontra-se disponível na *intranet* em duas plataformas, no SIGGNR e no SIGSIRESP, em que na primeira é possível ter acesso a toda a informação geográfica, bem como a algumas pesquisas rápidas que facilitam o acesso à informação. No caso do roubo de cobre, através de duas pesquisas, é possível ter a posição da ocorrência.

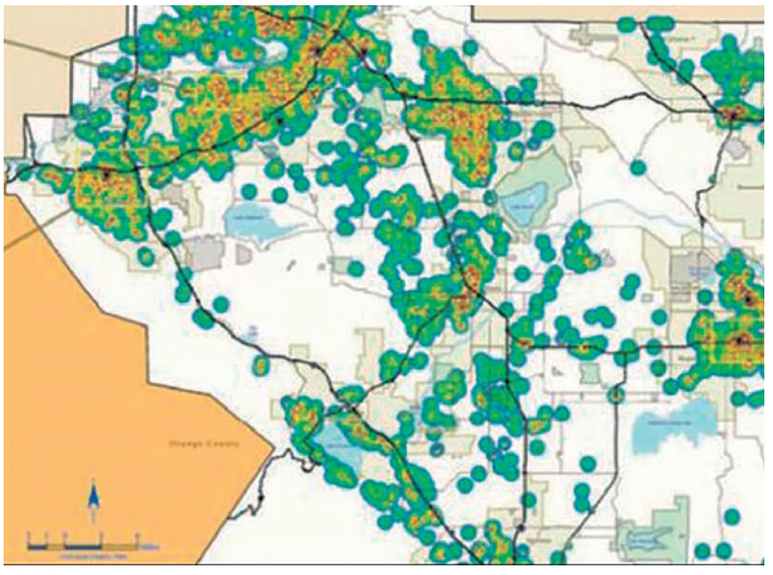
No que concerne à sinistralidade, é importante referir que é exequível obter as coordenadas, tendo a via e o respectivo km, tal como o oposto também é executável.

No SIGGNR encontra-se ainda informação sobre a divisão administrativa e variadíssima informação auxiliar que vai enriquecer as características da área de intervenção da GNR, bem como auxiliar na construção dos perfis geográficos.

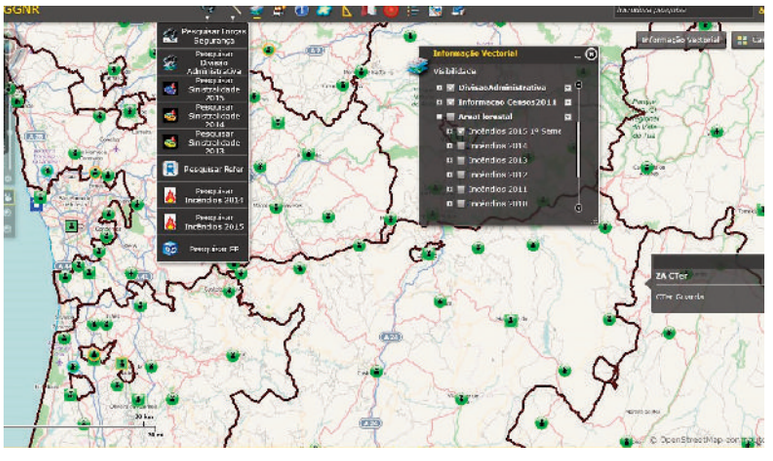
No SIGSIRESP, além da informação disponível no SIGGNR, encontra-se informação mais crítica, tal como informação da residência segura, idosos em segurança, etc.

Os Sistemas de Informação geográfica são, pelo exposto, fundamentais em forças de Segurança como a Guarda Nacional Republicana, por serem um sistema de apoio à decisão.

Eng.ª SÓNIA ALEXANDRE



O SIG é usado para determinar o nível de risco de crimes sexuais em Riverside County, California



Pesquisas passíveis de realizar no SIGGNR

Pesquisar as coordenadas do km 55 da EN4

Resiliência, velocidade e interoperabilidade

"Uma organização é uma combinação de esforços individuais que tem por finalidade realizar propósitos coletivos. (...) inatingíveis para uma pessoa."

Maximiano, 1992

Histórico

A GNR identificou há muito, a necessidade de um Sistema de Informação Policial com a finalidade de inovar, simplificar, desmaterializar e tornar mais eficientes, todos os "processos funcionais", em todas as áreas da atividade operacional da GNR, garantindo uma superior qualidade de atendimento ao cidadão, bem como uma racionalização da gestão que permita a redução de custos global, a adoção de uma administração eficaz e a efetiva materialização de redes de partilha e de interoperabilidade com outros organismos nacionais e internacionais. Em harmonia com o Plano Tecnológico do Ministério da Administração Interna (MAI), a implementação global do Sistema Integrado de Informações Operacionais de Policia (SIIOP) da GNR, enquanto tecnologia de Informação e conhecimento de suporte à atividade operacional, constitui-se como uma necessidade estrutural essencial ao funcionamento e modernização desta Força de Segurança.

Neste contexto, o SIIOP permite com especial enfoque:

- A simplificação e modernização administrativa, prestando ao cidadão um serviço policial de excelência;
- Maior capacidade de prevenção e de combate à criminalidade;
- Reengenharia e simplificação dos "processos de negócio"/"processos de trabalho" da GNR, segundo critérios de eficiência e eficácia organizacionais;
- Normalização e desmaterialização documental, através do uso intensivo de tecnologias de informação e comunicação;
- Redução de custos de contexto, Rentabilização dos meios financeiros do Estado, através de um retorno do investimento, traduzido numa futura redução de custos diretos de operacionalização (despesa de pessoal e meios materiais) e num grande incremento da qualidade do serviço prestado (maior eficiência na prevenção e no combate à criminalidade e às infrações em geral);
- Potenciar a interoperabilidade entre Sistemas de Informação de vários parceiros que contribuem para a segurança nacional e internacional;
- Redes de colaboração e de conhecimento;
- Uma forte componente de formação e qualificação dos recursos humanos.

Devido ao facto do "Sistema de Forças" da GNR se encontrar implementado e a operar ao longo do território nacional (abrangendo mais de 94% da área do País), num rol muito diversificado de áreas de atuação, é premente e estruturante para os interesses superiores do Estado e dos Cidadãos, potenciar a atuação da GNR e a prestação dos seus serviços de segurança, através da adoção de novas tecnologias de informação e de novos paradigmas de administração pública.

A Velocidade e a Resiliência

A nível nacional, o reforço da segurança constitui-se como um desígnio premente que só poderá ser atingido com a modernização tecnológica das suas Forças de Segurança e uma sólida formação de todos os seus agentes. Neste âmbito, o SIIOP está implementado e a funcionar em real, nos Comandos Territoriais do Porto, Faro, Lisboa, Setúbal, Viseu, Aveiro, Coimbra e Braga. Em 2015, foi lançada uma nova fase de implementações que adicionou os Comandos Territoriais de Évora, Beja, Portalegre e Castelo Branco à lista apresentada, ficando a faltar seis Comandos, com perspetiva de arrancar a fase de implementação em três a cinco comandos, ainda em 2015.

A situação geral das Tecnologias de Informação e Comunicação ao longo do Dispositivo da GNR, é marcada ainda por insuficiências na utilização de sistemas de informação, enquanto instrumento de suporte aos processos de trabalho, tanto na área administrativa, como na área operacional. Paralelamente, existe uma enorme quantidade de informação policial que a GNR elabora em suporte de papel, que não é totalmente registada informaticamente num sistema de informação.

Essas carências resultam fundamentalmente, do subinvestimento verificado neste domínio em anos anteriores. As insuficiências e inadequação dos sistemas de informação são espelhadas em défices de informação de gestão, resultando numa complexidade e morosidade dos processos que, sendo baseados em papel e tendo um baixo grau de automatização, obrigam a uma maior necessidade de afetação de recursos humanos à sua execução e a uma consequente perda de fiabilidade na transmissão e no acesso à informação.

A não implementação completa do SIIOP compromete a qualidade dos serviços prestados ao cidadão, o tratamento e análise da informação, coordenação e partilha de informação com outros organismos nacionais e internacionais, racionalização e sustentabilidade de custos, a otimização e agilização dos "processos de negócio" da GNR e, consequentemente, a prevenção e manutenção da ordem e tranquilidade públicas, o combate à criminalidade e às infrações do foro contraordenacional.

A infraestruturação de todos os quartéis do dispositivo dos Comandos Territoriais e, consequente-

mente, a migração de todos os equipamentos para a Rede Nacional de Segurança Interna (RNSI), que suporta as redes de dados do MAI, vieram trazer a capacidade de implementação e expansão do SIIOP a todos os quartéis da GNR, bem como aos restantes serviços suportados pela rede, como o correio eletrónico e a *intranet*.

Ao longo dos anos, a par da insuficiente infraestruturação das instalações e da GNR, e a correspondente ligação à RNSI, a velocidade da comunicação de dados na referida rede tem vindo a ser melhorada e encontra-se hoje melhor ajustada às necessidades e a suportar outros serviços, como as chamadas de VoIP - voz sobre IP (*Internet Protocol*), apenas suportadas pela RNSI, sem necessitar de passar pela rede pública.

Resiliência é um termo que, primeiramente, foi utilizado na física, significando todo e qualquer material que apresentasse a propriedade de retornar à sua estrutura física depois de sofrer uma pressão externa. Posteriormente, a ecologia e a psicologia apropriaram-se deste conceito. Na ecologia utilizam-no referindo-se às estruturas vivas que, mesmo sofrendo com alterações de grande magnitude no ambiente, são capazes de se adaptar a estas mudanças. E na psicologia, como o que explica a capacidade de superar traumas por alguns indivíduos e por outros não. Neste contexto, é visto como um comportamento que diferencia pessoas resilientes de não resilientes.

A resiliência também é definida como a união de dois componentes principais: a vulnerabilidade e a capacidade adaptativa. A vulnerabilidade é medida pela facilidade com que uma organização passa de um estado de equilíbrio para o desequilíbrio, após um evento inesperado. A capacidade de adaptação é medida através do grau de mudança exigido da organização, após esses eventos.

A GNR é claramente, uma organização resiliente. Os constrangimentos e obstáculos que se têm colocado, infelizmente, nos longos anos de implementação do SIIOP, não conseguiram que esta instituição secular se desviasse dos propósitos e da importância da existência de um sistema estratégico com as caraterísticas intrínsecas ao SIIOP e mantivesse os esforços contínuos para atingir o objetivo final.

A interoperabilidade no futuro

Num mundo marcado pela necessidade de fazer chegar, de forma cada vez mais rápida, toda a informação a quem dela necessita, a disponibilização dessa mesma informação por parte das diversas polícias assume um caráter de segurança nacional e internacional. Recorde-se que, tendo por base a utilização das novas tecnologias, no âmbito da interoperabilidade, o SIIOP, na sua plenitude, é um excelente instrumento de gestão, permitindo armazenar, organizar, manipular e cruzar informação com segurança, rapidez e atualização constante.

No passado, no âmbito do Protocolo SICOP (Sistema de Coordenação Policial), decorreram estudos com vista à implementação duma Partilha de Informação Criminal entre os diversos Sistemas de Informação Policiais dos principais Órgãos de Polícia Criminal (Guarda Nacional Republicana, Polícia de Segurança Pública e Polícia Judiciária).

Este objetivo foi operacionalizado pela Plataforma de Intercâmbio de Informação Criminal (PIIC), desenvolvida para o Sistema de Segurança Interna (SSI) e apresentada em 2013, pelo Secretário-Geral do SSI, para o qual o SIIOP está preparado para contribuir.

O SIIOP permite ainda, o estabelecimento de plataformas colaborativas pan-europeias que promovem a cooperação entre as estruturas dos Estados-Membros, nomeadamente, na área da segurança, que é fundamental para fazer face às ameaças emergentes.

Constitui-se ainda, como um objetivo estratégico para a GNR, a interoperabilidade entres os seus diversos sistemas de informação. O SIIOP, como um dos sistemas nucleares da GNR, terá funcionalidades de interoperabilidade para permitir que determinados processos automatizados por outros sistemas de informação da GNR possam pedir e enviar dados para o SIIOP, bem como, processos

do SIIOP possam fazer pedidos e enviar informação para os outros sistemas de informação da GNR.

O SIIOP é, efetivamente, o sistema estratégico de suporte à atividade operacional da GNR e a resiliência desta organização vai garantir, num futuro muito próximo, a globalização da utilização do SIIOP, decorrente da formação e implementação em todo o dispositivo territorial, e a adaptação do SIIOP às necessidades, resultado da experiência da operação do sistema nos últimos dez anos e da previsão de um aumento do investimento direto no SIIOP, planeado para 2016.

Ainda relativamente ao SIIOP, é necessário frisar-se que os grandes sistemas, ao nível internacional, são desenvolvidos sobre tecnologias "standard" orientadas para sistemas corporativos, especialmente direcionados para a recolha e análise de informação, os quais detêm elevada capacidade de interoperabilidade, sendo para isso utilizadas arquiteturas tecnológicas do tipo SOA (*Service Oriented Architecture*) que permitem a troca de informação com qualidade, em massa e com altos índices de segurança. A este nível, na Guarda, apenas o SIIOP está dimensionado e capacitado a interoperar neste tipo de arquiteturas com entidades externas nacionais e internacionais.

É premente garantir a partilha e a troca de informações entre os diversos atores, através dos seus sistemas de informação. Nesta ótica, a GNR deve materializar e operacionalizar de forma célere, um "Sistema Corporativo de Informação" que permita uma visão holística e comum da informação operacional em todo o seu dispositivo de forças, materializando um ponto de interoperabilidade único com outros sistemas nacionais e internacionais. Tal desígnio exige um investimento adequado em recursos humanos e tecnologia.

Major RICARDO BESSA

Centro de Comando e Controlo Operacional - CCCO

O Centro de Comando e Controlo Operacional (CCCO) foi criado no ano de 2003, por despacho do Excelentíssimo Comandante-Geral Interino, exarado na informação n.º 56 de 01 de abril de 2003, da 3.ª REP/CG/GNR.

A sua primeira regulamentação foi concretizada através da NEP/GNR 3.49 (3.ª REP) de 04 de abril de 2003, estabelecendo esta, que o CCCO funcionava na Sala de Operações da 3.ª Repartição, tendo como missão, a par de outras que viessem a ser definidas, dar resposta às solicitações dos CCCO das Unidades (Brigadas Territoriais), aos pedidos de consulta das bases de dados efetuados por todo o dispositivo da Guarda e estabelecer a ligação com a Sala de Situação do Gabinete Coordenador de Segurança/MAI.

Foi estabelecido que o funcionamento do CCCO seria em permanência, sendo assegurado, em regra, no período normal, pelo efetivo da Sala de Operações (militares das 2.ª e 3.ª Repartições) e no período de atividade reduzida, por um guarda da 2.ª e 3.ª repartição nomeado para o efeito.

Seria da Competência do Oficial de Dia ao Comando Geral ou do Sargento de Dia à sala de Operações, na ausência do Oficial de Dia, assegurar o correto funcionamento do CCCO.

Em consequência da restruturação da Guarda Nacional Republicana e através do despacho 23021/08, do Excelentíssimo Tenente-General Comandante-Geral, publicado no Diário da República n.º 242, de 16 de dezembro de 2008, o CCCO foi colocado na dependência direta do Excelentíssimo Comandante do Comando Operacional.

Em 21 de janeiro de 2009, o Excelentíssimo Tenente-General Comandante-Geral, através de despacho exarado na proposta de diretiva sobre o funcionamento do CCCO, que deu lugar à diretiva 01/10/CCCO, e que ainda se encontra em vigor, estabeleceu a forma como o CCCO executa a sua missão.

A permanente evolução das tecnologias e sistemas informáticos veio, por um lado, permitir ao CCCO cumprir com mais eficiência e eficácia as atribuições e competências que lhe estão conferidas e por outro, veio tornar mais exigente às Unidades implementadas em todo o território nacional, a célere transmissão das notícias ou informações ao Comando Superior da Guarda.

A criação de Salas de Situação nas Unidades tornou-se uma necessidade imperativa no processo evolutivo de Comando e Controlo Operacional para o acompanhamento da evolução dos Sistemas de Gestão Operacionais e resposta às exigências atuais.

A NEP/GNR- n.º 3.53 de 21 de dezembro de 2012, do Comando Operacional/ Direção de Operações, veio definir as atribuições e competências do Centro de Comando e Controlo Operacional e das Salas de Situação das Unidades, contribuindo desde logo, para a compreensão da necessária simbiose entre ambos.

No princípio do ano de 2015, a Guarda Nacional Republicana, através do Comando Operacional, deu início a um projeto de modernização e criação de novas estruturas para o seu Centro de Comando e Controlo Operacional.

O "velho" Auditório do corredor de D. Nunes Alvares Pereira deu lugar ao "novo" CCCO.

O "novo" Centro de Comando e Controlo Operacional ficou localizado em instalações com elevada visibilidade e adequabilidade, exigindo normativos, requisitos funcionais e operacionais tempestivos, que possibilitam transformar o CCCO numa estrutura de excelência, assente na modernidade tecnológica, evolução procedimental e na melhoria contínua processual.

As boas práticas internacionais são orientadas para a interoperabilidade de técnicas, tecnologias e sistemas que efetuam o tratamento, fusão e partilha de informação, com consequências diretas nos processos, fluxos de informação e tipologia de recursos humanos envolvidos neste tipo de estruturas.

Os benefícios que se alcançam com esta mudança de metodologia são: a fusão tempestiva da informação; uma visão global comum de ocorrências e meios; dados estatísticos de qualidade acrescida, validados e concentrados. É o fundamental garante da qualidade da informação transmitida.

A operacionalização da nova estrutura do CCCO teve de compreender um conjunto de atividades de reorganização processual, aprovação de normativos, recrutamento, seleção, nomeação, colocação, formação e treino de pessoal.

1 - Garantir a monitorização, permanentemente, da atividade operacional da Guarda, e auxiliar na resolução dos incidentes que ultrapassam as capacidades e competências operacionais das Unidades;
2 - Realizar a monitorização e gestão de todos os sistemas de bases de dados de apoio à atividade operacional (SIIOP, SG2S, SGOSITREP, SGR, SGS, SGRUAF, SQE, SIG-GNR, SIGSIRESP, SIS II e outras que venham a ser criadas ou implementadas);
3 - Monitorizar os OCS, relativamente a notícias que possam influenciar a conduta das operações;
4 - Monitorizar a situação meteorológica com o objetivo de informar o dispositivo sobre a ocorrência de condições atmosféricas adversas que possam afetar ou prejudicar o normal desenvolvimento da atividade operacional;
5 - Monitorizar o trânsito rodoviário nacional por forma a manter atualizada a informação relativa às condições de circulação na rede viária, recorrendo ao SGR, à troca de informações com o Centro de Controlo Operacional da Brisa, Centro de Controlo e Informação de Trânsito das Infraestruturas de Portugal e OCS;
6 - Garantir o funcionamento permanente da linha "Azul de Trânsito", disponibilizando informações relativas a vias interditas ou condicionadas, sinistros rodoviários e condições de circulação;
7 Assegurar, de forma atempada, a troca de informação operacional com as Salas de Situação (SSit) dos Comandos das Unidades;
8 - Garantir a introdução e atualização dos dados referentes aos transportes de órgãos/produtos biológicos e teleassistência no âmbito da Violência Doméstica;
9 - Garantir o encaminhamento dos pedidos de localização celular, de acordo com os procedimentos em vigor;
10 - Manter informado o Comandante Operacional sobre o desenrolar da atividade operacional na Zona de Ação (ZA) da Guarda, dando-lhe conhecimento de imediato, nos casos de crimi-

nalidade e sinistralidade graves, assim como outros incidentes/ocorrências passíveis de provocar alarme social e projeção mediática relevante, nomeadamente, as que envolvem militares da Guarda;

11 - Manter informado o Comandante Operacional sobre atentados terroristas ocorridos no espaço da União Europeia ou fora deste, sempre que possam existir alvos de interesse nacional atingidos ou cidadãos nacionais, entre as vítimas. Da mesma forma, aplica-se os mesmos pressupostos nas situações de calamidade ou desastres naturais;

12 - Disponibilizar internamente toda a informação e dados estatísticos referentes à atividade operacional e respetivos resultados em coordenação com as Direções do Comando Operacional;

13 - Assegurar o relacionamento com a sociedade civil e Órgãos de Comunicação Social (OCS), prestando os esclarecimentos possíveis e adequados que lhe sejam solicitados referentes à atividade operacional, nomeadamente, os que estejam relacionados com a criminalidade violenta e grave, sinistralidade rodoviária e traficabilidade das vias de comunicação terrestre, entre outros.

Hoje o CCCO é composto por três salas: a Sala de Operações Correntes (SOC), que funciona ininterruptamente com um efetivo de oito militares; a Sala de Apoio às Operações Correntes (SAOC), concebida para funcionar no conceito de "*Fusion Center*" e a Sala de Brífingue diário, ou Sala de Crise, nas situações em que o Comando pretenda acompanhar ou assumir o comando de incidentes ou ocorrências mais graves.

O Centro de Comando e Controlo Operacional (CCCO) é assim, um órgão de apoio ao Comando e controlo operacional que visa garantir a permanente monitorização e acompanhamento da atividade operacional da Guarda e auxiliar no processo de tomada de decisão.

Tenente-Coronel JOÃO NORTADAS

FUSION CENTER
Informações, Comando e Controlo no apoio à decisão

O Valor da Liderança

No mundo atual, o processo de globalização tem sido caraterizado por um conjunto de transformações políticas, económicas e sociais de natureza complexa e interdependentes. A opacidade e imprevisibilidade dos riscos e ameaças constituem, no presente, enormes desafios no domínio da segurança, em diversas dimensões. **Novas configurações das ameaças** impõem uma abordagem integrada e multidisciplinar de diversos atores, sejam eles públicos ou privados.

Com efeito, diversos líderes mundiais e instituições internacionais têm reconhecido a necessidade de desenvolver e **adotar um novo paradigma de informações[1] e inteligência**[2] que promova a integração e partilha efetiva de informações entre diversas agências, forças de segurança, instituições públicas e privadas. As carências e responsabilidades em identificar, prevenir, monitorizar e reprimir atividades criminais e terroristas são comuns, tais como as soluções o deverão ser.

Todavia, desenvolver e promover a partilha efetiva de informações entre diversas agências e instituições não constitui uma tarefa simples. Para além de uma **liderança forte e assertiva**, carece do compromisso, dedicação e confiança de um conjunto unificado de pessoas que acreditem no **poder colaborativo**.

[1] Em sentido estrito - dados constituirão informações quando possuírem um significado e compreendermos o seu contexto e relacionamento.

[2] **Inteligência** - É o saber que advém da integração relacional e análise prospetiva de várias informações (em sentido estrito), padrões, causalidades e princípios associados que resultam na obtenção cognitiva e analítica de conhecimento e compreensão, os quais valorados em função do julgamento e experiência, possibilitam a elaboração de predições futuras.

Como resultado deste processo, os Estados Unidos da América (EUA), através do *U.S. Department of Justice (DOJ)* e *U.S. Department of Homeland Security (DHS)*, desenvolveram uma iniciativa e projeto de partilha de informações e inteligência denominado *"FUSION CENTERS"*.

Os *fusion centers* reúnem todos os parceiros relevantes para maximizar a capacidade de prevenção e resposta a atos de terrorismo e ilícitos criminais. Trata-se de uma formação multidisciplinar e interinstitucional unificada entre diversas agências e forças de segurança, órgãos e instituições de segurança pública, saúde, transportes, bombeiros e setor privado. Atualmente já existem 78 *fusion centers* só nos Estados Unidos da América.

***Fusion Center* - Um novo paradigma de informações e inteligência**

"*Turning Information and Intelligence into Actionable Knowledge*"[3]. O **conceito de fusão** emergiu da necessidade e constitui-se como o processo fundamental para promover e facilitar a partilha de dados e informações relacionadas com a segurança interna e criminalidade. Define-se pelo processo global de gestão do fluxo de informação e inteligência em todos os níveis e setores do governo e da indústria privada. Todavia, está para além da implementação de um **centro de informações e inteligência** ou criação de uma rede de computadores. O **processo de fusão** apoia a implementação de programas de prevenção, de resposta, de gestão de incidentes e seus efeitos, orientados pelas informações e análises de risco. Por outro lado, potencia as sinergias indispensáveis para a resolução de conjunturas e acontecimentos imediatos ou emergentes relacionados com as ameaças.

A fusão de dados envolve a troca de informações de diversas fontes – públicas e privadas, sendo que, mediante a sua análise conjunta, poder-se-á obter

[3] Conceito de Fusão ((DHS), U.S. Department of Justice (DOJ) and U.S. Departement of Homeland Security, 2005, p. 10

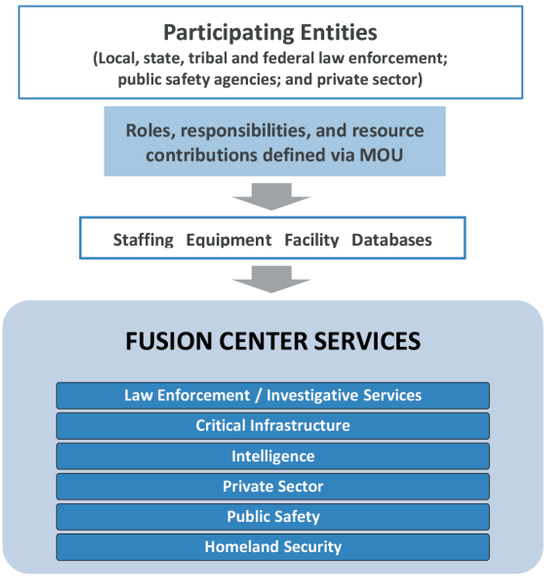


Figura 1 – Fusion Center Components
Fonte: Adaptado de *Fusion Center Guidelines* (2006)

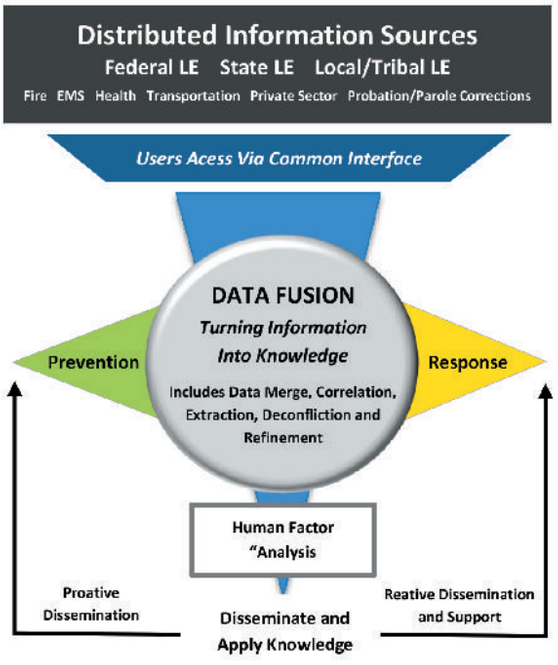


Figura 2 – Fusion Process
Fonte: Adaptado de *Fusion Center Guidelines* (2006)

informações relevantes e acionáveis. A integração entre segurança pública e componentes do setor privado no processo de fusão, promove a interoperabilidade de conhecimentos e experiências de diversos especialistas em assuntos que podem ajudar na identificação de ameaças. O processo de fusão transforma essa informação em conhecimento oportuno e operável, permitindo uma reavaliação contextualizada dos dados e informações preexistentes com novos dados, a fim de fornecer atualizações.

Não constitui a intenção dos *fusion centers* promover a união de todas bases de dados públicas e privadas num único sistema central. Apenas proporcionar a sua consulta, recolha, análise e disseminação, através dos diversos responsáveis e intervenientes, em função da pertinência, riscos, ameaças, necessidades de segurança pública ou índole criminal. O **produto** desta partilha será armazenado pela entidade executante, de acordo com as políticas do centro, competências legais ou exigências de privacidade.

O que é então um *Fusion Center*? – "É o esforço de colaboração entre duas ou mais instituições que fornecem recursos, conhecimentos e informações ao centro, com o objetivo de maximizar a sua capacidade de detetar, prevenir, investigar e responder a atividades criminosas e terroristas".

"*A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources.*" ((DHS), U.S. Department of Justice (DOJ) and U.S. Departement of Homeland Security, 2005, p. 2).

O **suporte para a atividade de um *Fusion Center*** depende dos processos e ciclos de inteligência e de fusão, através dos quais a informação é recolhida, integrada, avaliada, analisada e divulgada. Todavia, é recomendável que a integração e recolha de dados públicos e privados se processem de forma virtual, através das redes e utilizando funções de pesquisa, salvaguardando a segregação de informações reservadas a determinadas entidades.

A **atividade principal de um *Fusion Center*** será manter uma perceção situacional consciente e um sistema alarmístico, suportado pela inteligência resultante do ciclo de produção informações, onde as

necessidades de informação oportuna são definidas e geradas, recolhidas, integradas, avaliadas, analisadas e disseminadas.

O processo de fusão não substitui ou replica os processos de produção de inteligência ou gestão da informação. Contudo, será através da, integração e alavancagem destes processos que se criarão sistemas de apoio na identificação oportuna de padrões e tendências que podem constituir uma ameaça emergente. As potencialidades são inúmeras.

As **fases do processo de fusão,** genericamente, correlacionam-se com o ciclo de produção de informações.

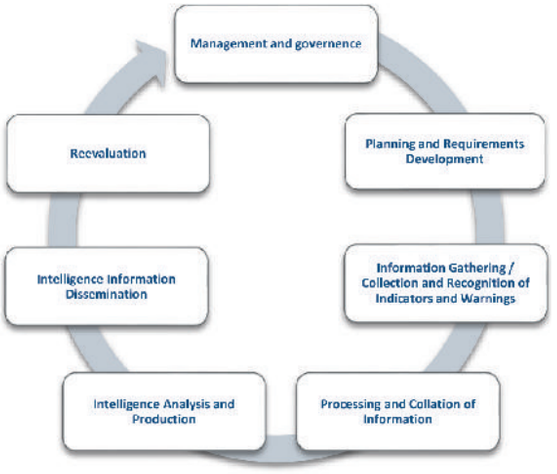


Figura 3 - Ciclo e Processo de Fusão

A **ênfase da fusão** assenta na identificação de ameaças e riscos emergentes, relacionadas com o terrorismo entre outras atividades criminosas, bem como no apoio e agilização das operações correntes.

Alguns dos **objetivos e funções** de um *Fusion Center* poder-se-ão resumir da seguinte forma:

- Constituir-se ponto de contato prioritário para participação de informação criminal ou terrorista às diversas forças de segurança, unidades contraterroristas e centros de comando e controlo operacional;
- Dinamizar a capacidade de integrar informações policiais e de inteligência;
- Identificar atempadamente, ameaças emergentes;
- Recolher, analisar e divulgar toda informação criminal, de modo a identificar padrões e tendências emergentes - avaliar e reavaliar o processo, novos dados, e as ameaças emergentes;
- Apoiar as capacidades de análise preditiva;
- Apoiar e agilizar as atividades correntes, constituindo uma resposta multidisciplinar e proativa na resolução problemas transversais e focalizados na comunidade;
- Viabilizar o desenvolvimento de um policiamento orientado pelas informações – *intelligence-led policing;*
- Adotar e aderir a uma estratégia nacional para avaliar as trocas de informações entre forças de segurança e diversos parceiros de serviços de informações ou de segurança interna;
- Servir como *HUB* de receção e disseminação de informações policiais preveniente dos diversos serviços, agências e forças de segurança;
- Manter uma avaliação de risco atualizada a nível nacional;
- Simplificar a prestação de serviços de emergência e não emergência;
- Maximizar os recursos disponíveis;
- um instrumento fundamental de monitorização operacional e apoio à decisão.

A atividade de um *fusion center* funda-se no conceito *intelligence-led policing*. Esta metodologia oferece reconhecidas vantagens para a segurança pública e privada, rasteando tendências criminais, possibilitando uma melhor articulação na prevenção e combate à criminalidade.

Proatividade em detrimento de reatividade. O processo fusão permite descrever, compreender e mapear a criminalidade, comportamentos e atuações criminais, efetuar escolhas e decisões sustentadas, empregar as táticas mais adequadas, maximizar recursos, desarticular a criminalidade grave e organizada, bem como suportar informações públicas ou inquéritos judiciais.

O *FUSION CENTER* DA GNR

Tendo por base os novos desafios, necessidades operacionais e ameaças, no âmbito da **Diretiva n.º 01/15/CO – CCCO de 18 de maio de 2015**, aprovada pelo Exmo. Tenente-General Comandante-Geral da Guarda Nacional Republicana, em 13 de julho de 2015, foi implementado o novo Centro de Comando e Controlo Operacional (CCCO) GNR.

A **instalação e operação do novo CCCO** exige normativos, requisitos funcionais e operacionais tempestivos que o permitam transformar numa estrutura de excelência, assente na modernidade tecnológica e evolução procedimental.

Com efeito, foi necessário assegurar a interoperabilidade de técnicas e implementação de tecnologias e sistemas que efetuem o tratamento, fusão e partilha de informação, com consequências diretas nos processos, fluxos de informação e tipologia de recursos humanos envolvidos neste tipo de estruturas. Os **benefícios** que se pretendem alcançar com esta mudança de metodologia são: a fusão tempestiva da informação; uma visão global comum das ocorrências e meios; dados estatísticos de qualidade acrescida, validados e concentrados; transformar rotinas associadas a tarefas de monitorização numa atividade exógena às Direções; e, libertar estas estruturas para incrementar atividades de planeamento e direção.

Figura 4 – Organização do novo CCCO GNR

A **implementação de um CCCO e *FUSION CENTER*** no Comando Operacional da GNR possibilitou à Guarda Nacional Republicana, no âmbito da sua **estratégia genética, operacional e estrutural**, desenvolver uma capacidade que não detinha, projetando-se para o futuro, mediante a criação de um instrumento de apoio à decisão, de comando e controlo operacional eficaz. A adoção de um modelo integrado de informações, de comando e controlo, numa única estrutura, constitui uma abordagem inteligível, eficiente e versátil. As potencialidades de uma sala desta natureza são imensas.

O ***FUSION CENTER* da GNR** é uma equipa multidisciplinar, constituída por elementos permanentes e de ligação proveniente das diversas estruturas funcionais e especialidades da Guarda, tendo por finalidade garantir a permanente monitorização, acompanhamento, análise e disseminação de informações públicas, policiais e criminais, em apoio das atividades e operações correntes, auxiliando no processo de tomada de decisão.

Resumidamente, a sua função primária consiste em manter uma perceção situacional consciente, a fusão e partilha tempestiva de informações, asseverando a sua interoperabilidade, validade e qualidade, tendo em vista a identificação de ameaças e eventos em tempo real, maximizando a oportunidade de intervenção e eficiência operacional pelas diversas estruturas funcionais.

No exercício da sua atividade, poderão consistir atribuições específicas do *FUSION CENTER*, designadamente:

1 - Constituir-se instrumento fundamental de apoio à decisão e monitorização operacional da Guarda;
2 - Assegurar a pesquisa, compilação, análise e disseminação de informações policiais e criminais críticas, entre outras informações, em apoio das atividades e operações correntes;
3 - Garantir a monitorização de toda a componente operacional através das diversas Plataformas de Sistemas Integrados e de Gestão Operacional;
4 - Servir como *HUB* (centro de partilha) de receção e disseminação de informações policiais proveniente dos diversos serviços, agências e forças de segurança;
5 - Constituir-se ponto de contacto privilegiado para participação de informação criminal ou terrorista, em coordenação com os órgãos técnicos;
6 - Integrar informações policiais e de inteligência;
7 - Antecipar e identificar atempadamente, ameaças emergentes, prevenir e monitorizar atividades criminais relevantes ou socialmente divergentes, em coordenação com os órgãos técnicos;
8 - Recolher, analisar e divulgar todas informações de modo a identificar padrões e tendências emergentes;
9 - Proceder à pesquisa, recolha e tratamento de informações provenientes de fontes abertas – *Open Source Intelligence* (OSINT), no âmbito das atribuições do *FUSION CENTER*;
10 - Proceder à pesquisa, recolha, análise e tratamento de informações e documentos provenientes de fontes abertas, instituições públicas ou privadas protocoladas – *Imagery Intelligence* (IMINT), no âmbito das atribuições do *FUSION CENTER*;
11 - Providenciar informações de natureza estratégica, operacional e tática focalizada nas atividades e operações correntes, em coordenação com os órgãos técnicos;
12 - Integrar e interpretar variáveis e dados resultantes de informações de natureza policial ou criminal com informação relevante, previamente estruturada e processada pelas diversas direções ou órgãos técnicos;
13 - Assegurar o apoio multidisciplinar, proativo e centralizado em atividades de resolução de problemas focalizados no cidadão, na qualidade do serviço prestado, ou em questões transversais à comunidade;
14 - Desenvolver capacidades de análise preditivas de apoio à decisão, maximizando a oportunidade de intervenção e eficiência operacional;

15 - Maximizar a colaboração, comunicação e capacidade integrada de vários recursos, serviços ou valências, minimizando redundâncias ou replicação de processos;
16 - Simplificar a prestação de serviços operacionais de emergência, não emergência e contingência;
17 - Integrar recursos tecnológicos, sistemas e pessoas;
18 - Manter e gerir, através dos diversos elementos e entidades, o acesso a um leque diversificado de bases de dados e sistemas de informação a disponibilizar em função da necessidade e pertinência, em tempo oportuno;
19 . Assente numa visão holística e integrada, manter a interoperabilidade de técnicas e procedimentos dos diversos elementos da sala, em coordenação com os respetivos órgãos técnicos;
20 - Colaborar para a identificação, análise e avaliação de riscos específicos associados ao cumprimento da missão da Guarda;
21 - Possibilitar o desenvolvimento de um policiamento orientado pelas informações – *intelligence-led policing*;
22 - Assegurar a conservação e tramitação de documentos classificados, em condições que garantam a sua integridade e segurança;
23 - Elaborar e difundir relatórios resultantes da atividade de informações;
24 - Promover, em articulação com o órgão técnico e determinações superiores, atividades de contrainformação e segurança;
25 - Manter, em coordenação com a Direção de Informações, o desenvolvimento e manutenção de um sistema integrado de informações;
26 - Monitorizar, recolher e analisar notícias e informações divulgadas nos órgãos de comunicação social (televisão, rádio, *Internet*), nas plataformas *online* e redes sociais com interesse para a GNR ou influência na conduta das atividades e operações;
27 - Responder a solicitações enviadas pelos cidadãos, bem como divulgar conteúdos e informações, através das plataformas *online* e redes sociais da GNR;
28 - Prestar serviços de apoio às atividades de investigação, gestão e técnicas nos domínios da proteção de dados, sistemas comunicação e informação, cibersegurança e recursos tecnológicos;
29 - Manter atempadamente informado e atualizado, o Comando Operacional da Guarda sobre qualquer notícia, informação, evento ou atividade pertinente para a segurança nacional e dos cidadãos em geral, para o desenvolvimento da missão da Guarda ou passíveis de provocar alarme social e projeção mediática relevante.

Decorrente da sua atividade, poderão ser produzidos os seguintes ***outputs***:

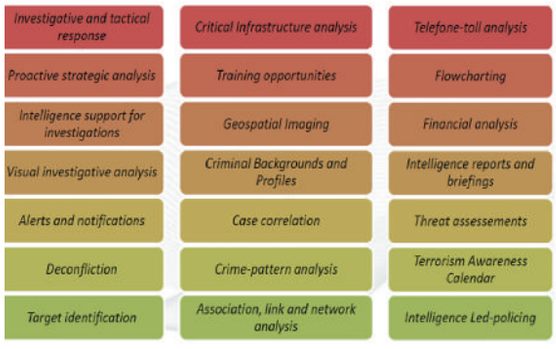


Figura 5 – *Intelligence Services and Products*

Desafios e Constrangimentos

A implementação de um *fusion center* desta natureza **constitui um processo evolutivo** que carece de um conjunto diversificado de recursos, técnicas, formação, tecnologias e sistemas adequados. Para que o seu desenvolvimento seja possível, é indispensável a colaboração, dinamização e empenhamento alargado de um conjunto diversificado de intervenientes e estruturas.

Todavia, muitos são ainda os **desafios e tarefas** a realizar:

- Definir os papéis e responsabilidades de todas as partes envolvidas;
- Definir e aprovar canais e fluxos de informação internos e externos;
- Definir expetativas, níveis de eficiência e como medir o seu desempenho;

- Definir a missão, metas, objetivos, políticas e regras de funcionamento, competências legais e exigências de privacidade do *fusion center;*
- Aprovação e implementação de regulamentação orgânica e funcional do *fusion center;*
- Desenvolver um manual de procedimentos que corresponda às necessidades do serviço;
- Prover a preparação, treino e formação técnica adequada aos militares que desempenham funções no *fusion center*;
- Adquirir ferramentas e sistemas analíticos e preditivos de *business inteligence;*
- Implementar um plano de avaliação periódica das diretivas e procedimentos, estimulando a purga de atuações desajustadas;
- Estabelecer um código deontológico e de conduta específico do *fusion center*.

No domínio tecnológico, para **transpor-se do plano operacional para o plano analítico**, é imperativo integrar todos sistemas de informação disponíveis em sistemas de *data warehousing,* extraindo, transformando e normalizando todos dados em *DataSmarts* estruturados, segundo determinadas concordâncias.

Subsidiariamente, é necessário a implementação de sistemas, algoritmos, *software* de *business intelligence* e *analysis* que permitam executar *data mining*, reconhecer padrões e causalidades, compreender os princípios e consequentemente, **predizer o futuro**.

O *FUSION CENTER* da Guarda visa apoiar as diversas estruturas funcionais da Guarda, potenciando sinergias e externalidades positivas, sempre em regime de complementaridade e subsidiariedade nas diversas áreas de estado-maior.

Pela natureza e indissociabilidade das suas atribuições, o *FUSION CENTER* deverá sempre ser chefiado por um Oficial Superior da Direção de Informações. Sempre que se justifique, para o desenvolvimento de determinado tipo de eventos, atividades ou operações, por determinação superior, o *FUSION CENTER* poderá ser temporariamente guarnecido por oficiais de ligação, técnicos ou especialistas de diversas unidades, serviços ou órgãos.

A implementação de um centro de informações constitui um dos pilares vitais para a vertente operativa da área de informações de qualquer instituição ou força de segurança.

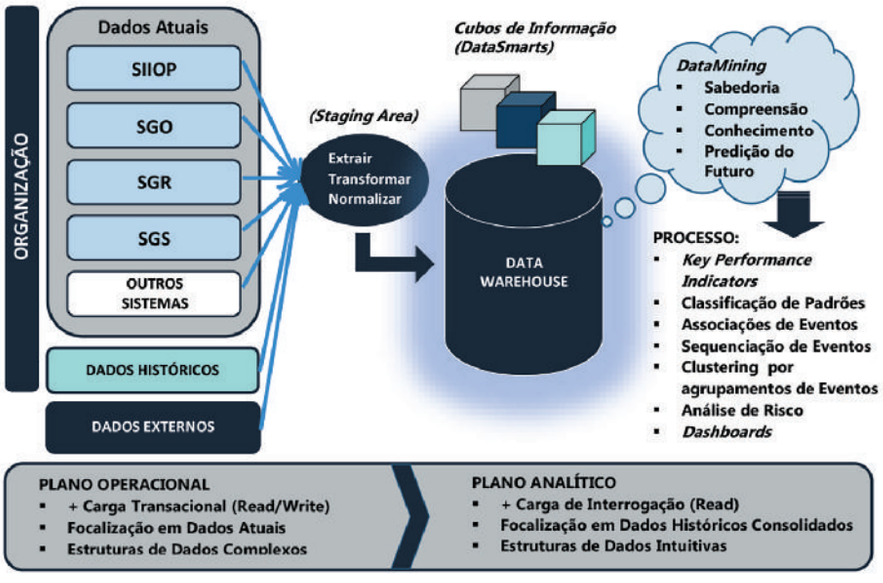


Figura 7 – Integração Sistemas de Informação em *DataWarehousing* Fonte: Adaptado de GTTSI GNR

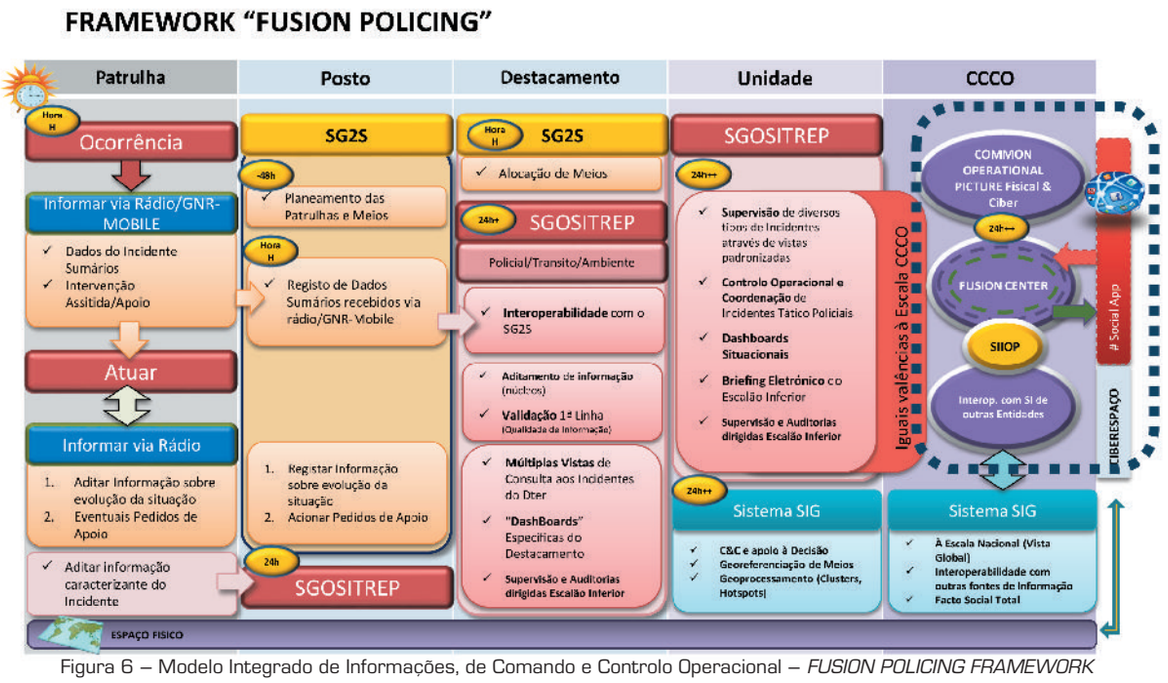


Figura 6 – Modelo Integrado de Informações, de Comando e Controlo Operacional – *FUSION POLICING FRAMEWORK*
Fonte: GTTSI GNR – Tenente-Coronel Paulo Santos

Sabemos que **o caminho é longo, mas forçosamente terá de ser trilhado**. Novas configurações das ameaças e exigências operacionais diversificadas impõem um novo paradigma de informações e *intelligence*. O *Fusion Center* constitui a resposta inteligível aos desafios que a GNR enfrenta numa nova Era, maximizando a oportunidade de intervenção e eficiência operacional pelas diversas estruturas. Inequivocamente, este é e será um poderoso instrumento de apoio à decisão, que em muito simplificará o exercício do comando e controlo operacional.

Capitão JOÃO MADALENO

BIBLIOGRAFIA

(DHS), U.S. Department of Justice (DOJ) and U.S. Departement of Homeland Security. (2005). *Fusion Center Guidelines - Developing and Sharing Information and Intelligence in a New Era.*

(DHS), U.S. Department of Justice (DOJ) and U.S. Departement of Homeland Security. (2009). *Fusion Center Technology Guide - DHS/DOJ Fusion Process Technical Assistence Program and Services.* EUA.

Ackoff, R. L. (1989). From Data to Wisdom. *Journal of Applied Systems Analysis, 16*, pp. 3-9.

Comandante-Geral da GNR. (19 de Julho de 2011). Despacho n.º 9634/2011.

Decreto Regulamentar n.º 19/2008 . (27 de Novembro de 2008).

Guarda Nacional Republicana - Comando Operacional. (18 de Maio de 2015). Diretiva Operacional n.º 01/15/CO - CCCO.

Ministério da Defesa Nacional - Exército Português. (2009). *PDE 2-00 - Informações, Contra-Informação e Segurança.*

Desenvolvimento Aplicacional na GNR

Sistemas de Informação e sua evolução

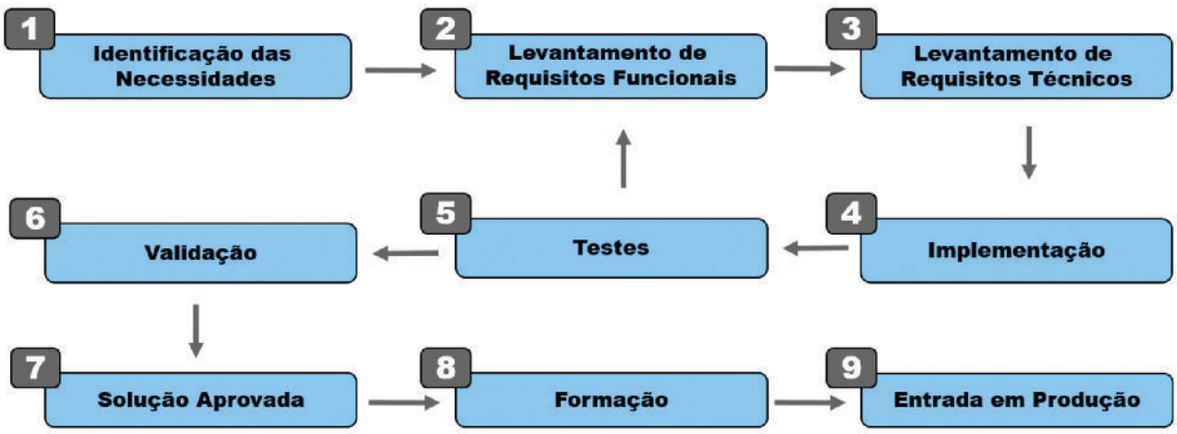
Um Sistema de Informação (SI) é um conjunto de recursos técnicos e humanos que proporcionam o armazenamento, processamento, distribuição e transmissão de informação útil para o utilizador, tendo em vista a otimizar o processo de apoio à tomada de decisão e o controlo dos recursos à sua disposição. Todos nós somos elementos fundamentais num SI, onde assumimos diversas funções. Desde a recolha de dados, à sua transformação em informação e a geração de conhecimento preditivo necessário para cumprir funções complexas na área da investigação e da informação policial. A transmissão desta informação pode ser simplesmente, efetuada de forma eletrónica (exemplo: *e-mail*, documentos em formato digital, entre outros) ou através de *software* específico, onde se armazena o tipo de informação que se pretende transmitir, para que os utilizadores tenham acesso a essa informação [exemplo: Sistema de Gestão Operacional (SGO), Sistema de Gestão Rodoviário (SGR), entre outros].

A implementação eficiente de um SI tem um papel muito importante, porque permite a desmaterialização do papel, simplifica os processos de trabalho, especialmente, os que são extremamente complexos, tendo como objetivo principal o de acabar com a carga burocrática ao nível organizacional, por forma a tornar o processo de consumo de informação simples e rápido, de modo que os utilizadores dos SI possam dar respostas rápidas e oportunas à sua cadeia hierárquica, prestando um serviço policial de qualidade superior ao cidadão.

Ciclo de desenvolvimento aplicacional

O ciclo de desenvolvimento aplicacional é materializado por um conjunto de fases distintas de trabalho que se sucedem de forma lógica, visando permitir de forma sistematizada e eficaz, a implementação de um Sistema Aplicacional (SA).

Existem diversos modelos de desenvolvimento aplicacional, cada um com as suas vantagens e inconvenientes, devendo ser adaptados à organização onde são utilizados. Em cada uma das fases intervêm entidades funcionais e técnicas com áreas e responsabilidades bem delimitadas. Não existe uma obrigatoriedade estática na ordem destas fases. Dependendo da situação, o modelo pode ser adap-



tado de uma forma dinâmica, permitindo adequar-se da melhor forma possível para resolver o problema existente.

O ciclo de desenvolvimento aplicacional exemplificado na figura 1 é constituído por nove fases. A 1.ª fase corresponde ao levantamento inicial das necessidades e à definição do âmbito da aplicação. Durante esta fase a entidade funcional (a entidade que possui necessidade de uma solução de *software*) identifica o âmbito do futuro SA, referindo as razões ou situações particulares que justificam a sua implementação, os objetivos que se pretendem atingir e o impacto que isso representa para a instituição.

Posteriormente, são levantadas pela entidade funcional uma lista de requisitos como por exemplo, os tipos de utilizadores, as funcionalidades da aplicação, os tipos de relatórios, os processos de trabalho, bem como a "lista dos campos" que irá conter o futuro Sistema, assim como as áreas ou módulos que irá comportar. Na fase de levantamento de requisitos técnicos, são modeladas e descritas pela entidade técnica, as especificidades e necessidades técnicas ao nível da arquitetura tecnológica, aplicacional e informacional.

Finalizando as fases de levantamento de requisitos passamos para a 4.ª fase, a fase de implementação. Esta fase consiste na criação da aplicação, concebendo, desta forma, o Sistema pretendido que espelha o levantamento dos requisitos funcionais e técnicos das fases transatas.

Uma aplicação pode dividir-se em diversas camadas, nomeadamente, a *interface* com o utilizador, a camada de negócio e a camada de dados (figura 2). Neste domínio, as tecnologias a serem implementadas e as linguagens de programação são diversas, diferentes entre si, e com diferentes implementações nas diversas camadas.

Depois de o Sistema ter sido desenvolvido, segue-se a fase de exploração do SA, num ambiente de testes mais aproximado à realidade, no qual o sistema irá ser operado (é conduzida pelas entidades funcionais e técnicas). Durante esta fase, poderão surguir alterações de requisitos funcionais, o que

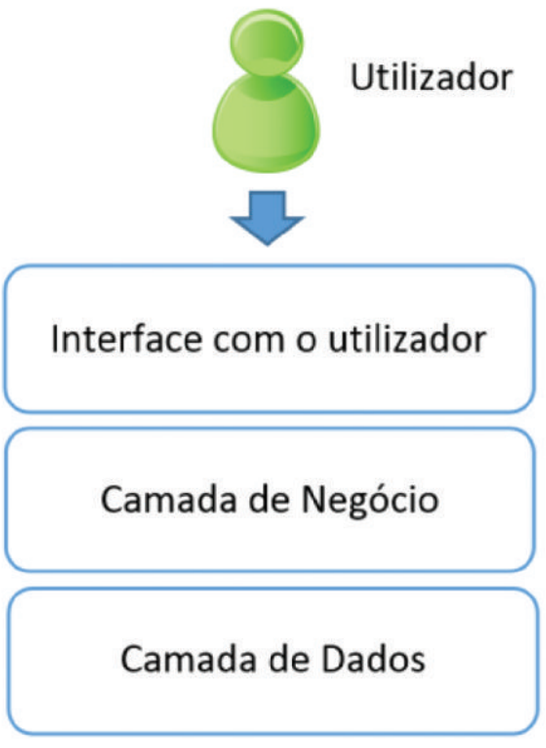


Figura 2 – Camadas de uma aplicação Web.

leva à alteração de requisitos técnicos e, por sua vez, a uma nova implementação dos novos requisitos.

Na 6.ª fase o Sistema é validado pela Entidade Funcional e Técnica por forma a garantir que a implementação corresponde aos requisitos funcionais e técnicos. Se a aprovação for positiva, passamos para a fase que corresponde a um período de formação de utilização do Sistema desenvolvido.

Na última fase, o Sistema entra em produção, correspondendo à exploração real. As posteriores ações de manutenção (evolutiva, adaptativa ou corretiva) deverão ser implementadas em primeiro lugar, em ambiente de desenvolvimento, podendo-se seguir a sua publicação em ambiente de qualidade (ambiente de testes).

É necessário ter em conta que um SA encontra-se em constante transformação para poder responder às necessidades do utilizador e por isso, o ciclo de desenvolvimento encontra-se em constante circulação.

Desenvolvimento aplicacional na GNR – Passado, Presente e Futuro

O desenvolvimento de um SA surge, fundamentalmente, por necessidades funcionais dos utilizadores/elementos de um de terminado SI, por forma a responder à otimização deste sistema onde estão enquadrados.

Havendo uma tentativa por parte da Guarda em otimizar os seus SI, onde os seus militares se enquadram, bem como em terminar com o suporte em papel, criar maior rapidez e fluidez na chegada de informação a todos os escalões com necessidade de informação, foram criados diversos Sistemas para atingir este objetivo. Nomeadamente, o Sistema de Gestão Rodoviária (SGR), Sistema de Gestão Operacional (SGO), Sistema de Transmissão de Mensagens (STM), Sistema de Gestão de Manutenção TIE (SGMTIE), SGO SITREP (corresponde a uma nova versão do SGO), Sistema de Gestão dos Relatórios de Utilização de Armas de Fogo (SGRUAF), Sistema de Gestão SEPNA (SGS), GNR Mobile, *intranet*, *site* oficial da GNR, entre outros. Todos estes sistemas foram desenvolvidos inteiramente com os recursos internos da Guarda, quer recursos humanos e materiais, dando primazia à utilização de tecnologias *open source* (tecnologias livres e gratuitas).

Os SI sofrem uma constante evolução e transformação ao longo dos tempos. Inicialmente, existiam apenas os meios de transmissão de informação tradicionais (papel, rádio, fax, telefone, entre outros). Depois, ocorreu uma evolução para um conjunto de SA específicos para determinadas áreas da Guarda, prevendo-se a futura integração dos vários sistemas em apenas um sistema único, sendo este um objetivo estratégico incluído no planeamento estratégico para 2020.

Mais do que uma evolução tecnológica e de imple-

Figura 3 – Software desenvolvido pela GNR.

áreas da Guarda, prevendo-se a futura integração dos vários sistemas em apenas um sistema único, sendo este um objetivo estratégico incluído no planeamento estratégico para 2020.

Mais do que uma evolução tecnológica e de implementação de funcionalidades num sistema integrado, é necessário saber como atingir este objetivo estratégico. Tendo em conta a eficácia do *software* desenvolvido por entidades externas à Guarda e o *software* desenvolvido internamente, devemos ou não efetuar o desenvolvimento de um sistema desta envergadura com os recursos humanos internos? Deve haver uma aposta nos recursos humanos internos para a área de desenvolvimento aplicacional? Um SI deve estar bem definido, tal como os seus processos de trabalho antes do início do ciclo de desenvolvimento aplicacional. Será que temos capacidade e conhecimento suficiente para efetuar/definir detalhadamente, estes processos?

A área de desenvolvimento aplicacional na Guarda possui escassez de recursos humanos. Mesmo com esta escassez, a Guarda demonstrou enumeras vezes ser capaz de desenvolver soluções à medida do utilizador, dando uma resposta eficaz no seu desenvolvimento. Para criar um sistema integrado e de grande envergadura, esta equipa certamente terá de crescer, com recursos humanos suficientes e formação adequada.

Antes de se iniciar qualquer desenvolvimento aplicacional é necessário, como já foi referido, existir um levantamento de requisitos funcionais. Estes requisitos têm de incluir, de uma forma clara, todos os processos de trabalho da própria organização ou entidade. Estes processos devem encontrar-se bem definidos e espelhar o modo de funcionamento da organização/entidade para que, desta forma, seja possível otimizar estes processos e iniciar o desenvolvimento aplicacional. Se estes processos se encontrarem deficitários ou inexistentes, deve ser trabalhado, junto das entidades funcionais, a definição e otimização destes processos.

Será, certamente, um desafio para a Guarda, mas a necessidade de reflexão e resposta às questões apontadas será fulcral para que este objetivo seja alcançado.

Tenente TIE MAURO MACHADO

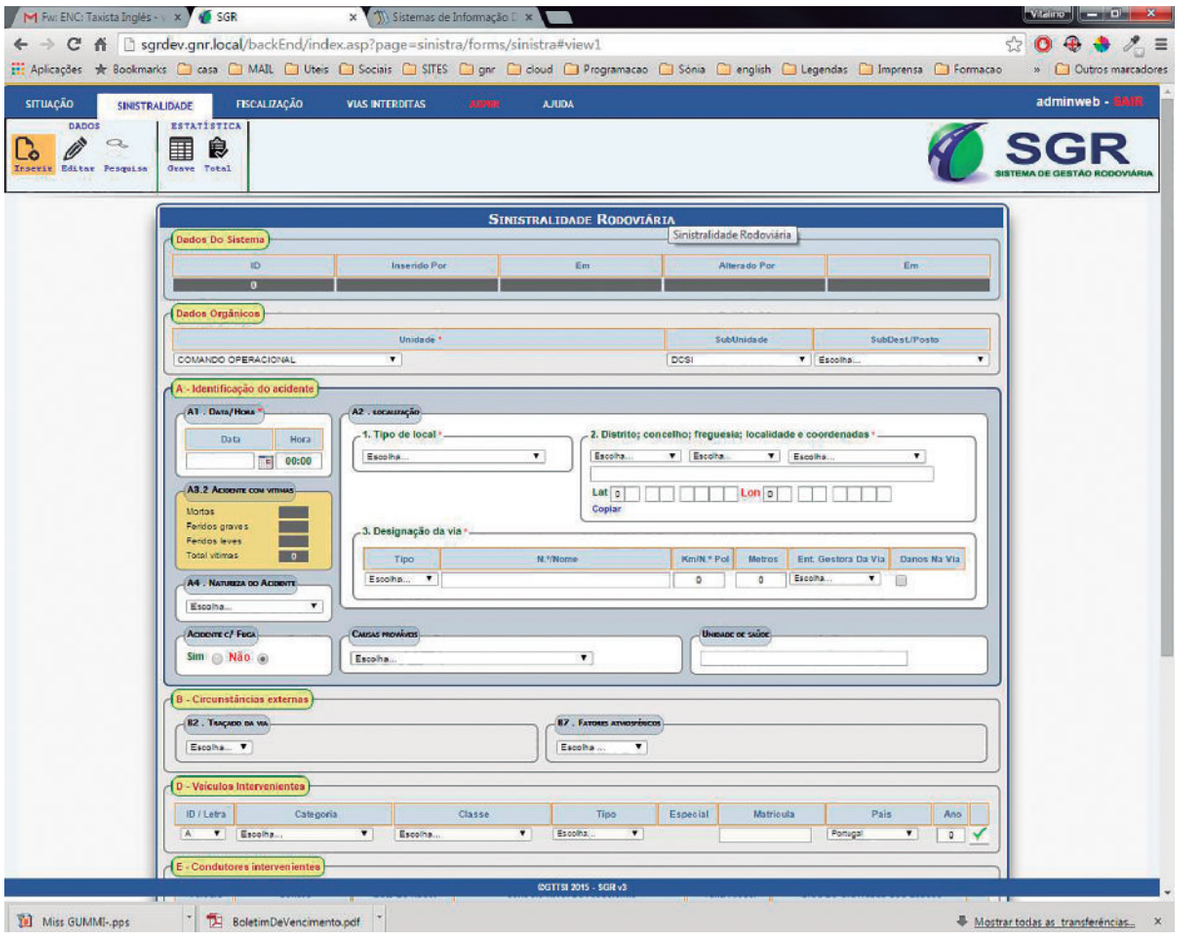
O SGR e o BEAV Eletrónico

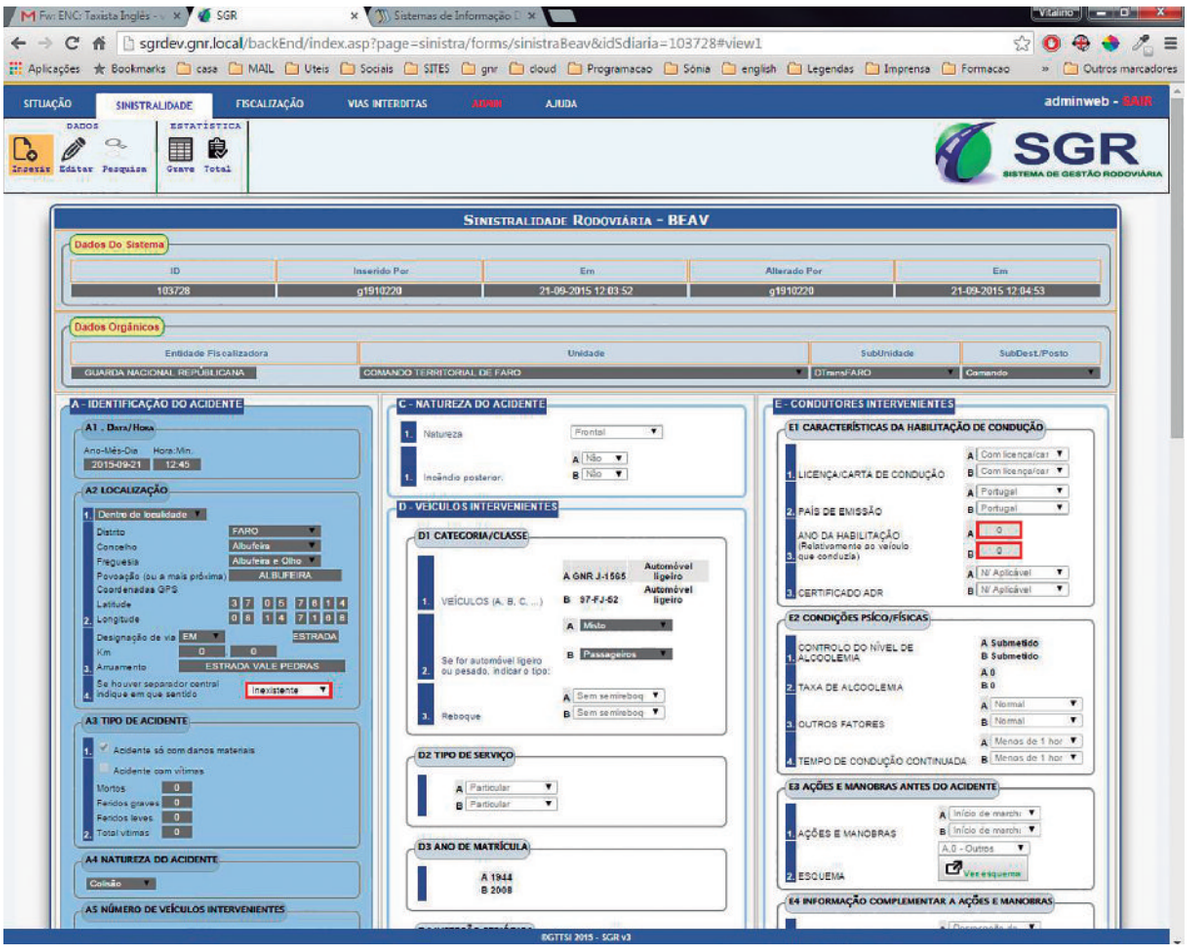
A informação tornou-se uma necessidade crescente para qualquer setor da atividade humana e é-lhe indispensável, mesmo que a sua procura não seja ordenada ou sistemática, mas resultante apenas de decisões casuísticas e/ou intuitivas.

Se a informação representa um património, esta agrega valor acrescentado. Assim, o uso dos recursos das tecnologias de informação (TI) de forma apropriada, implica utilizar ferramentas, sistemas ou outros meios que façam das informações um diferencial. Além disso, é importante procurar soluções que forneçam resultados realmente relevantes, isto é, que permitam transformar as informações em algo com valor maior, sem deixar de considerar o aspeto económico.

As organizações, ao atuar no mundo global, estão em estado de "necessidade de informação" permanente, a vários níveis, pelo que a informação constitui o suporte de uma organização e é um elemento essencial e indispensável à sua existência. A aceitação deste papel pelos dirigentes destas pode ser um fator perentório para se atingir uma situação de excelência: quem dispõe de informação de excelência, fidedigna, em quantidade adequada e no momento oportuno, adquire vantagens competitivas. Contudo, a sua escassez ou inexistência dá aso a tomada de decisões erróneas ou inoportunas.

Por conseguinte, a Guarda Nacional Republicana (GNR), como entidade fiscalizadora, desenvolveu um sistema de informação denominado Sistema de Gestão Rodoviária (SGR) que visa a recolha sumária de dados do fenómeno da sinistralidade rodoviária, ser-





vindo de suporte à avaliação das medidas a adotar à investigação, ao apoio à estatística e à definição de programas e estratégias, visando melhorar a segurança rodoviária a nível nacional e local.

Os dados depositados neste sistema têm por base a obtenção e utilização dos recursos de forma eficiente, satisfazendo os três níveis: estratégico, tático e operacional. Neste sentido, à medida que descemos na pirâmide hierárquica organizacional, a especificidade aumenta, pois é necessário resolver problemas mais específicos, enquanto ao nível de topo, as preocupações são mais gerais, afetando a generalidade das funções.

Consequentemente, tornou-se necessário evoluir no sentido de garantir a fiabilidade e qualidade do SGR quanto aos atrasos, faltas e/ou incoerências ou erros no seu preenchimento. Estas falhas têm repercussões no rigor das estatísticas realizadas com base nestes dados, podendo pôr em causa a credibilidade deste sistema de informação. Foram já desenvolvidas várias versões deste sistema, encontrando-se atualmente em fase de testes, a sua versão 3.

Se o SGR é a principal fonte de dados sobre a atividade fiscalizadora rodoviária da GNR, servindo de suporte ao diagnóstico da situação nacional neste domínio específico, tornou-se necessário incluir neste sistema todos os dados relevantes e inerentes àquela atividade.

O Boletim Estatístico de Acidentes de Viação (BEAV) é um instrumento de notação estatística, preenchido pelas entidades fiscalizadoras, sempre que tomam conhecimento da ocorrência de um acidente de viação, tendo em vista recolher dados que permitam retratá-lo o mais concreto possível.

A finalidade do BEAV é permitir caraterizar as circunstâncias em que ocorrem os acidentes de viação, bem como os utentes e veículos envolvidos. Foi imperativo desenvolver mais um módulo para suporte de

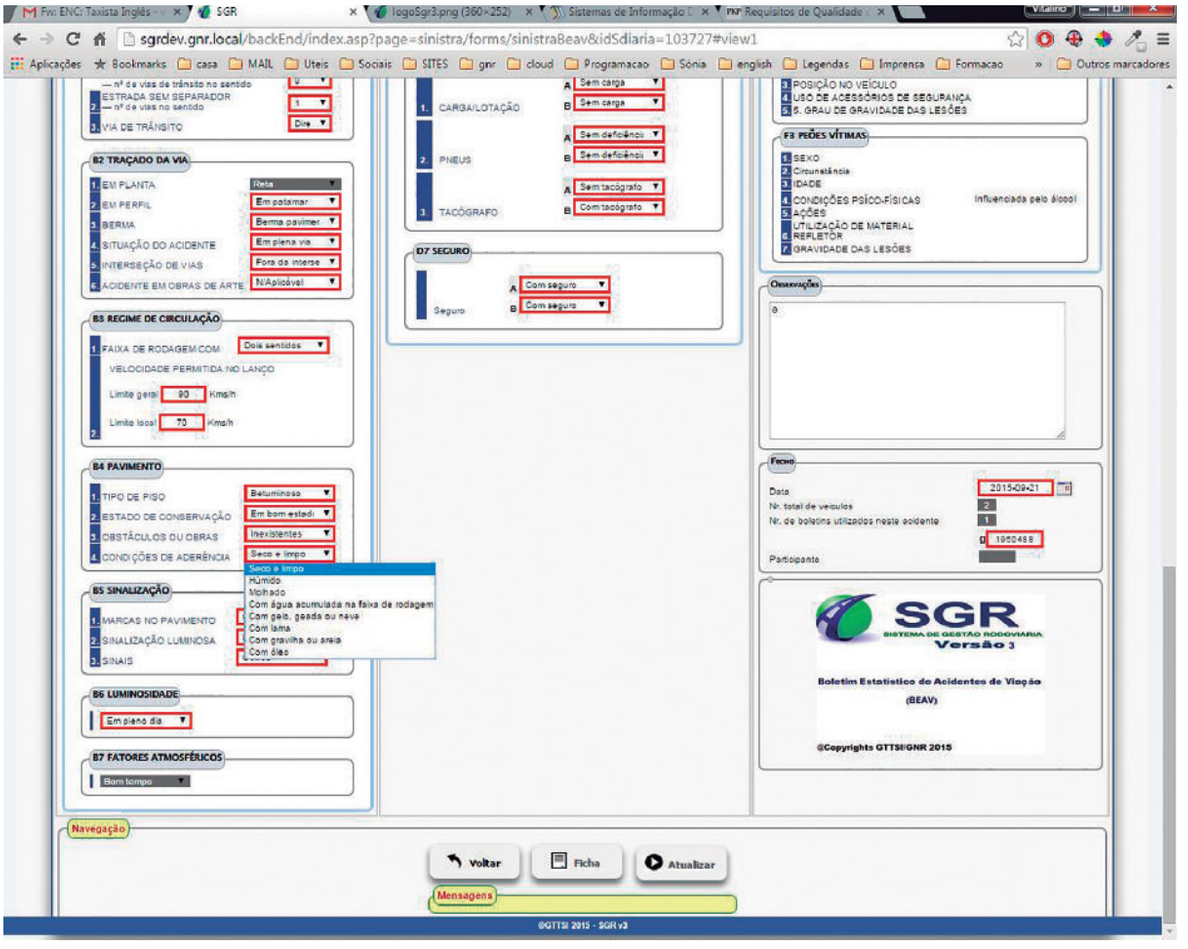
registo do BEAV na área da sinistralidade do SGR, respeitando um princípio basilar dos sistemas de gestão: os mesmos dados só devem ser inseridos nos sistemas uma única vez.

Assim sendo e a título de exemplo, no registo de acidentes de viação do qual só resulte danos materiais, o BEAV fica automaticamente preenchido com os dados já inseridos na ficha sumária. No caso de que resulte vitimas, torna-se necessário preencher o BEAV na sua totalidade. Contudo, alguns campos já se encontram automaticamente preenchidos com os dados anteriormente inseridos. O seu preenchimento obedece ao primado da usabilidade.

O SGR, enquanto plataforma *web*, é desenvolvido à medida das necessidades da GNR, desempenhando um papel de apoio na articulação das várias áreas que o constituem, com os sistemas envolventes e relacionando-se através da partilha de dados, com sistemas de outras entidades, na medida em que efetua o processamento de dados provenientes de múltiplos utilizadores, permitindo obter informação útil e em tempo real, apto para modelar dados que permitam a sua exportação simples, tornando-se assim, numa ferramenta útil à gestão e à tomada de decisão, de modo a permitir atuações imediatas e adequadas a cada situação.

O SGR, enquanto sistema de informação do âmbito das tecnologias da informação, não é apenas sinónimo de modernidade. É, acima de tudo, uma necessidade dos novos tempos. Afinal, os dados sempre existiram, mas não com a atual dimensão e características.

Sargento-Ajudante VITALINO GOMES



O novo *site* oficial da GNR (www.gnr.pt)

A Guarda, tendo-se consciencializado desde a 1.ª implementação do seu *site* oficial em 2000, da importância da *internet* como força motriz de inovação, donde emergem todo o género de atividades e relações sociais, tem vindo a redefinir, ao longo de seis versões sucessivas, o seu *site* oficial em termos tecnológicos, organizativos, ao nível de conteúdos e de serviços policiais. Ao longo de 15 anos, tem sido essa a matriz de autossuficiência da GNR, no âmbito do desenvolvimento aplicacional de todo o género de aplicações *web* internas e externas.

Atualmente, encontra-se em fase de finalização a 7.ª versão do *site* oficial da GNR que representa uma natural evolução da atual versão e que tem como objetivos principais:

- Potenciar as relações de "Proximidade com o Cidadão", aumentando a usabilidade do atual *site*.
- Ser diferenciador, materializando uma imagem mais "arrojada e dinâmica" da instituição, transmitindo uma ideia de modernidade.
- Apresentar conteúdos *web* mais intuitivos, mais fáceis de apreender e de dominar.
- Prover uma forma mais fácil de acesso à informação e aos serviços de segurança *online*;
- Disponibilizar uma maior quantidade de informação policial alinhada com as expetativas de segurança do cidadão.
- Apresentar um aspeto gráfico mais apelativo, em termos de *design* e de conteúdos gráficos, onde se promove uma imagem de uma Força de Segurança moderna;
- Disponibilizar uma melhor navegabilidade, usabilidade e aparência visual que provoca melhores experiências positivas do utilizador.
- Garantir mecanismos eficientes de proteção e segurança contra ciberincidentes delituosos, tendo como especial referência, os relatórios de segurança remetidos pela tutela.

Em termos tecnológicos, o *site* assenta nas mais modernas tecnologias de HTML5 e na linguagem de programação ".net". Será, contudo, necessário frisar-se que o *site* oficial não é apenas um "resultado tecnológico", mas sim a conjugação articulada de esforços que se desenhou entre a entidade técnica e as diversas entidades funcionais da GNR. Estas, executaram um trabalho diligente e cuidado na reunião e na atualização de conteúdos que foram inseridos nesta nova versão. Frise-se que este trabalho de contínua atualização de conteúdos será sempre necessário assegurar, dadas as constantes necessidades e expetativas informativas legítimas que o Cidadão tem, relativamente a assuntos de natureza policial e de segurança.

A realçar-se que a presença de uma instituição na *internet* representa uma projeção sem precedentes, da sua imagem e do seu papel na Sociedade. Assim, por mérito próprio, a Guarda tem sido sempre capaz de desenvolver e manter um *site* oficial que promovesse a sua imagem e que simultaneamente, fosse uma forma de acesso privilegiado a serviços e informações, caraterizadoras duma Força de Segurança que visa reforçar em permanência, as relações de proximidade com a Sociedade de Informação e do conhecimento.

1º Sargento PAULO MARQUES

LINUX – Levantar do Véu

Quando se ouve a palavra "Linux", muitos começam a questionar o que será que significa... Será uma nova aplicação? Uma marca de computadores? Um tipo de monitor? Ou será que é um "bicho-de-sete-cabeças"?

Para desmistificar este conceito tem de se perceber em primeiro lugar, o que é um Sistema Operativo (SO): no fundo, é um conjunto de programas e instruções desenhados para gerir os recursos de *hardware* disponíveis e permitir com que o *software* (normalmente designado por aplicações) seja executado. Por outras palavras, o Sistema Operativo é o *software* que controla os recursos de *hardware*.

Partindo deste princípio, colocam-se várias questões: Existem vários tipos de Sistemas Operativos? O Windows é um Sistema Operativo? Onde é que aqui encaixa "esse tal" Linux?

As respostas não podiam ser mais diretas: existem diversos tipos de Sistemas Operativos, sendo que uns estão mais adaptados a determinadas funcionalidades que outros. O Sistema Operativo com maior utilização na GNR é o Microsoft Windows ®, o que não implica que outros Sistemas Operativos não se encontrem de momento, em funcionamento na instituição.

Seguindo este raciocínio, pode então concluir-se que o Microsoft Windows é sim, um Sistema Operativo, tal como outros que também são sobremaneira conhecidos

Possivelmente, neste momento, deve estar a interrogar-se acerca da utilização ou não, deste sistema operativo... O que é que faz este SO ser diferente? Na realidade, a resposta a esta questão poderia ser muito complexa, caso entrássemos em preciosismos técnicos, mas surpreendentemente, a resposta é muito simples: este SO é (na sua base) gratuito!

Linux – Introdução Histórica e Distribuições

Quando surgiu então este Sistema Operativo? Tal como podemos encontrar em [1], em 1991 surgiu a primeira versão à qual podemos, efetivamente, chamar Linux. Foi inicialmente desenvolvida por Linus Trovaldis e desde aí, tem vindo a evoluir a um ritmo estonteante. Atualmente, existe toda uma comunidade de programadores e entusiastas que contribuem para a evolução do sistema base (*kernel*) e que criam *software* à medida deste Sistema Operativo. Para além destes, existem empresas que moldaram o sistema base às suas necessidades e que vendem versões mais "empresariais" que têm suporte desse tipo.

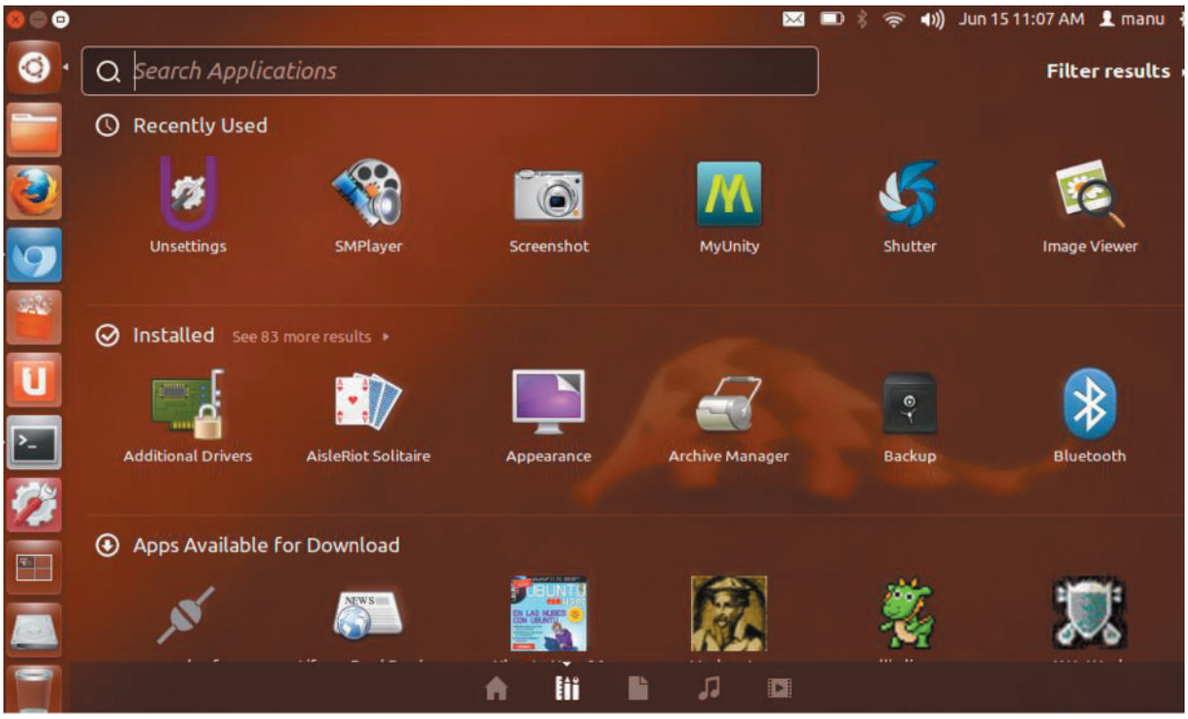
Com esta variedade toda de programadores e entusiastas do Linux, existem muitas distribuições deste Sistema Operativo que mais não são, que derivações do Sistema Operativo original e que mantêm a base do mesmo. Certamente que já ouviu falar em nomes como: Ubuntu, Debian, RedHat ou Mint. Uma lista mais pormenorizada das distribui-

Apple OSX

Linux

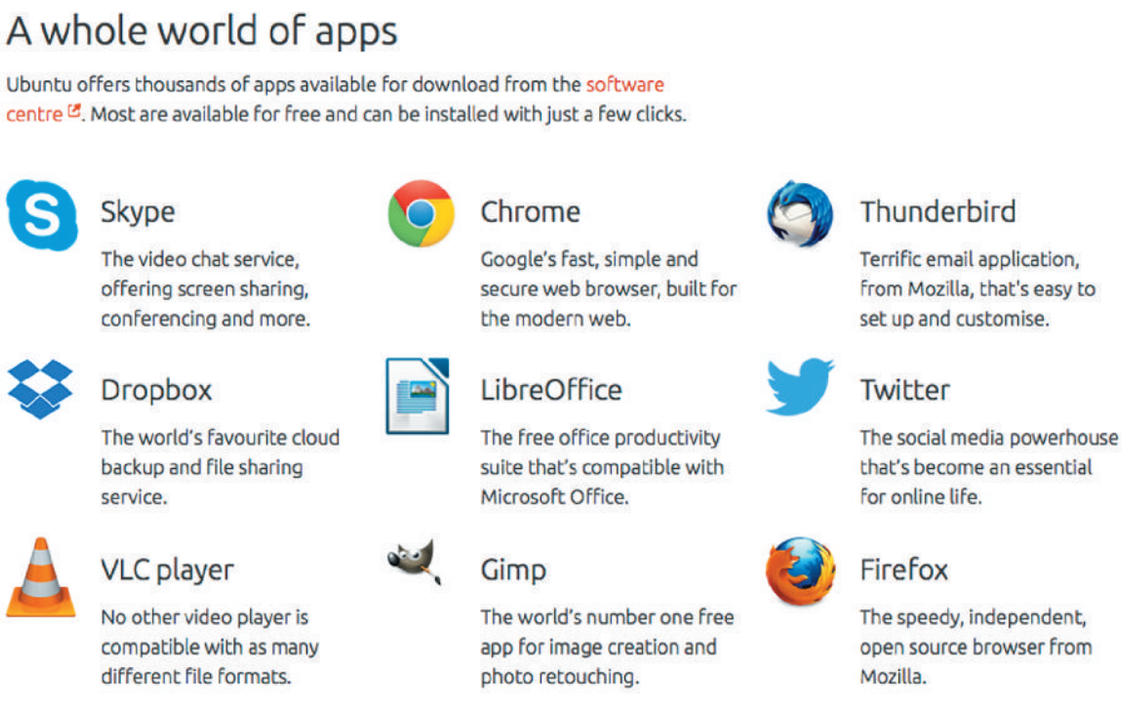
ções Linux disponíveis pode ser encontrada no *site* http://www.distrowatch.com.
Atualmente, estão listadas neste *site* cerca de 760 distribuições diferentes! Para que tenha perceção das ramificações existentes, atente ao seguinte link:http://futurist.se/gldt/wp-content/uploads/12.10/ gldt1210.svg
Todas estas distribuições são no fundo, conjuntos de pacotes de *software* desenhados para realizar tarefas mais específicas e que estão adaptadas a diferentes tipos de utilização: umas foram desenhadas para serem operadas enquanto estações de trabalho, outras para tratamento gráfico, outras para operar em rede, etc., etc...
Seguem então abaixo, breves súmulas acerca de distribuições conhecidas (e outras interessantes):

Ubuntu – ótimo para começar:
Ubuntu é uma distribuição Linux que é uma ramificação de outra distribuição (a Debian).
Esta distribuição é ótima para utilizadores inexperientes e que nunca tenham tido contato com *Linux*. Trata-se de uma distribuição otimizada para utilização no seu próprio computador, pelo que é intuitiva e dispõe da maioria das ferramentas necessárias para o trabalho/lazer do dia-a-dia pré-instaladas, tais como: ferramentas de processamento de texto e cálculo, navegadores *web*, *e-mail* e ferramentas de reprodução de vídeo/som [2].
Além destas caraterísticas, tem *firewall* e antivírus



Fonte: http://1.bp.blogspot.com/-vl6_q7kvg-0/T9rKsj7nNsI/AAAAAAAAD7M/zavqrokda-M/s1600/ubuntu1204-alteprecisepangolin.png

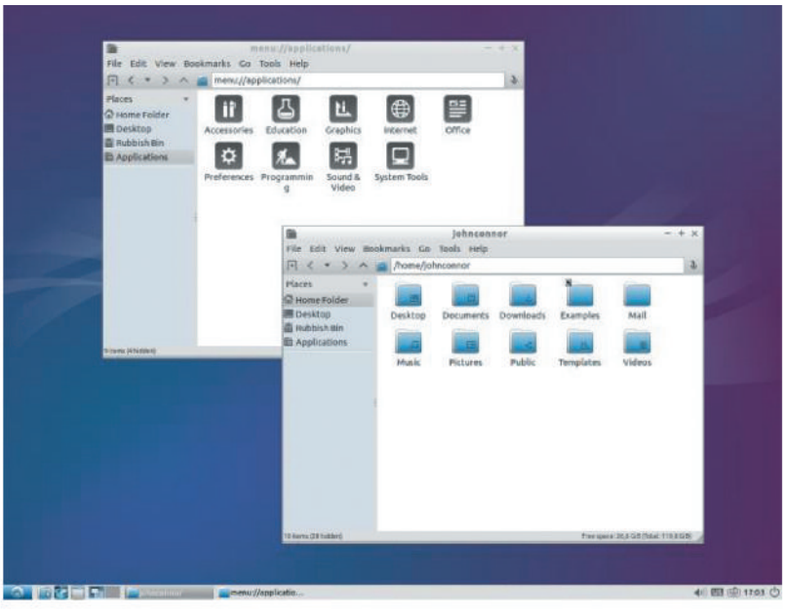
embebidos e suporte de longa duração, (LTS - *Long Term Support*), o que faz com que seja suportado pelo menos, durante cinco anos e está disponível em 40 línguas, entre elas, a língua portuguesa.
Esta distribuição, à semelhança de muitas outras, tem disponíveis aplicações/programas bastante úteis que são utilizados à larga escala, como se pode ver pela figura abaixo, cuja imagem foi retirada do *site* oficial:



Fonte: www.ubuntu.com/desktop

Lubuntu – Reaproveitar o seu computador mais velho

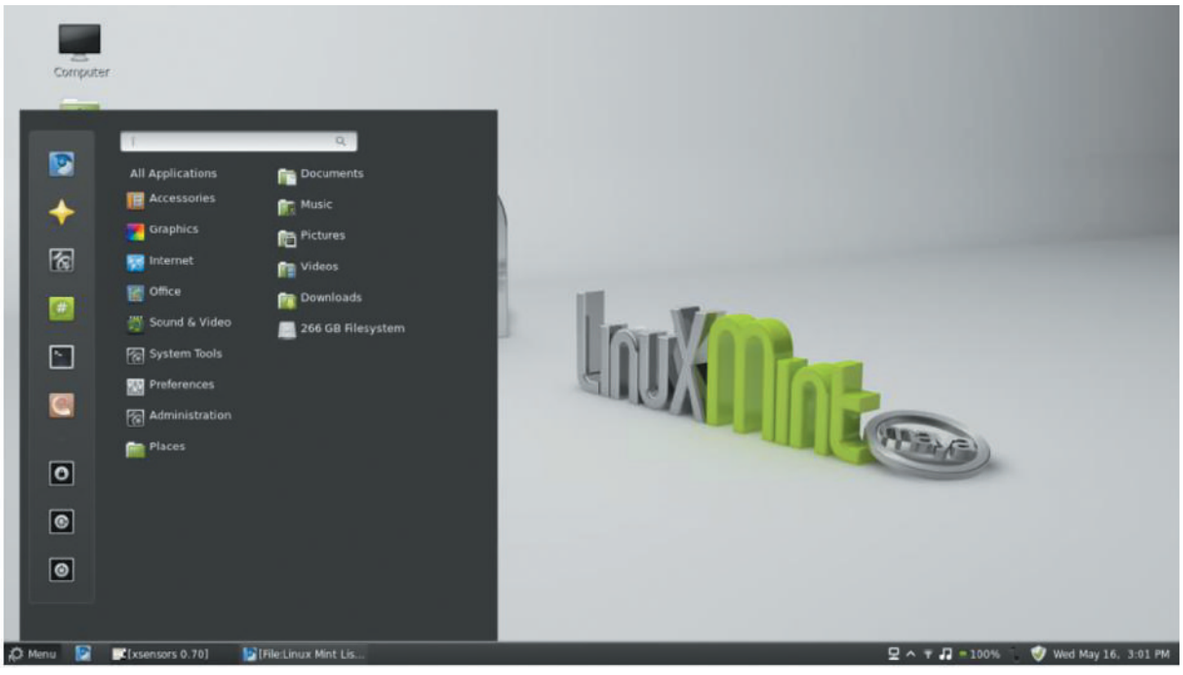
Esta distribuição [3] tem como lema "*lightweight, fast, easier*" que significa "leve, rápido e mais fácil". Com estas três palavras resume-se toda uma distribuição, uma vez que o que a carateriza é o facto de ser focada na velocidade de execução e na poupança de energia. Caso tenha algum computador mais velho em casa, esta será a distribuição mais indicada.



Fonte: http://1.bp.blogspot.com/-vl6_q7kvg-O/T9rKsj7nNsI/AAAAAAAAD7M/zavqrokda-M/s1600/ubuntu1204-altepreciseпangolin.png

Mint

Esta distribuição [4] é uma das que mais tem recebido aderentes nos últimos tempos e a prova disso, é o seu lugar na tabela classificativa encontrada em www.distrowatch.com. Foi desenhado para ser moderno e elegante, de forma a ser poderoso e fácil de utilizar.



Fonte: http://www.linuxmint.com/

Linux – Futuro na instituição

Atualmente, no que diz respeito ao futuro da utilização de distribuições Linux na GNR, muito pode ser dito. As restrições orçamentais que todos vivem fazem-se sentir na área dos sistemas operativos e face a isto, as soluções *opensource* começam a ser usadas no seio da nossa instituição e com uma taxa de crescimento regular. Atualmente, nos serviços centrais, são alguns os servidores que operam com este Sistema Operativo, sem que isso seja notado pelos utilizadores. Refiro-me a aplicações como o SG2S ou o SGO-SITREP, que estão atualmente assentes em tecnologias deste tipo.

Quanto à futura utilização em estações de trabalho, muito tem de ser feito de forma a percorrer o caminho até à implementação. As configurações associadas a este tipo de tecnologia requerem formação e capacidade de adaptação, face a toda a infraestrutura tecnológica que sustenta os Sistemas da GNR. Mas, mais difícil que os desafios tecnológicos será a gestão da mudança, materializando-se nesta questão: como se pode fazer uma implementação Linux no dispositivo, sem que os utilizadores vejam a sua forma de trabalhar comprometida? Não é uma tarefa impossível, mas implica que haja reflexão no caminho a seguir e nas opções que existem espalhadas pela comunidade, bem como cativar os utilizadores a fazerem parte de algo que já faz parte do dia-a-dia de milhões de pessoas por esse mundo fora.

Tenente TIE RICARDO AUGUSTO

Referências:
[1] Andrew S. Tanenbaum, "Modern Operating Systems", Pearson Education International, 2009.
[2] Ubuntu Desktop, [Online]. Disponível em: http://www.ubuntu.com/desktop [Acedido em: Setembro 2015].
[3] Lubuntu, [Online]. Disponível em: http://lubuntu.net/ [Acedido em: Setembro 2015]
[4] Mint, [Online]. Disponível em: http://www.linuxmint.com/ [Acedido em: Setembro 2015]

SIIOP – Formação e Qualidade

O que é o Sistema Integrado de Informações Operacionais de Polícia (SIIOP)

O SIIOP é um Sistema informático, baseado num repositório único, centralizado e alargado a todo o dispositivo, que permite à Guarda o suporte à Decisão/Acção, baseado em informação alargada e em tempo real, bem como a uniformização de procedimentos em toda a hierarquia da Guarda Nacional Republicana.

Responsabilidades do Gabinete SIIOP

- Implementação e acompanhamento da utilização do sistema em todo o dispositivo da Guarda;
- Supervisionar a formação SIIOP ministrada ao efectivo.

Implementação do SIIOP

Neste momento, o SIIOP está implementado e a funcionar em real, nos Comandos Territoriais do Porto, Faro, Setúbal, Aveiro, Viseu, Lisboa, Coimbra, Braga, Évora, Beja, Portalegre e Castelo Branco (12 Comandos).

No Comando Territorial de Santarém encontra-se a decorrer a fase de formação de utilizadores.

"As resistências à mudança fazem parte dos próprios processos de mudança".

De facto, é sociologicamente explicado que, no âmbito de qualquer reestruturação ou introdução de novos métodos que impliquem alterações substanciais numa determinada organização, as resistências à mudança fazem parte dos próprios processos em curso. Contudo, no que ao SIIOP diz respeito, tais resistências poderão ser atenuadas, se os militares utilizadores forem devidamente acompanhados em todos os processos e etapas da formação e implementação do sistema.

A necessidade de se implementar o SIIOP na GNR

O SIIOP tem a finalidade de inovar, simplificar, desmaterializar e tornar mais eficientes, todos os "processos funcionais" nas áreas da Actividade Operacional da GNR, garantindo uma superior qualidade de atendimento ao cidadão, bem como uma racionalização da gestão que permita a redução global de custos, a adopção de uma administração eficaz e a efectiva materialização de redes de partilha e de interoperabilidade com outros organismos nacionais e internacionais.

Formadores do Comando Territorial de Évora

Formadores do Comando Territorial de Castelo Branco

«Devido ao facto do "Sistema de Forças" da GNR se encontrar implementado e a operar ao longo do território nacional, num rol muito diversificado de áreas de actuação, é premente e estruturante para os interesses superiores do Estado e dos cidadãos, potenciar a actuação da GNR e a prestação dos seus serviços de segurança, através da adopção de novas tecnologias de informação e de novos paradigmas de administração pública em que se inclui o *eGovernment*».

A formação SIIOP na GNR

A Guarda, através da coordenação do Gabinete SIIOP da Direcção de Informações, com as diferentes Áreas e Comandos envolvidos, ao proceder à implementação de um sistema como o SIIOP, está a assumir um compromisso com a inovação e a redireccionar todo o seu potencial para responder às prioridades tecnológicas marcadas pelas necessidades operacionais dos seus utilizadores.

A opção por se ministrar formação do SIIOP a todos os militares da GNR, tanto nos diversos Comandos, como na Escola da Guarda, tornou-se um factor decisivo na aceitação do sistema, contribuindo decisivamente para o progressivo e impresindível êxito do projecto, diminuindo-se assim as sempre existentes resistências à mudança. Sendo o potencial humano da GNR um elemento basilar para que o SIIOP seja cada vez mais, uma realidade e um sucesso em toda a sua dimensão, é considerado fundamental que a formação seja assegurada a todo o efectivo, de forma consistente e uniforme. Na Escola da Guarda (EG), unidade de formação por excelência, é ministrado um módulo de formação SIIOP a todos os militares da GNR, quer aos cursos iniciais de formação de Guardas, quer aos diversos cursos de promoção.

Aos militares já colocados nos diversos Comandos Territoriais, distribuídos por todo o país, é ministrado um plano de formação do sistema ao longo de uma semana, contemplando as diversas áreas do trabalho administrativo e operacional da GNR. Este plano de formação é ministrado por militares do efectivo do próprio Comando, com a vantagem de conhecerem os formandos, a necessidade de maior ou menor enfoque em determinadas matérias, devido às especificidades da criminalidade local, e evitar deslocamentos "forçados" que poderiam motivar uma menor predisposição para a formação.

Os formadores dos Comandos receberam uma formação de formadores, ministrada por militares do Gabinete SIIOP, que se pretende consigam transmitir a experiência pessoal e profissional adquirida ao longo dos anos, aliada aos conhecimentos técnicos da aplicação, conjugação indispensável para o êxito das formações. Estes formandos ficam com a responsabilidade de formarem os restantes utilizadores do Comando.

A par da formação SIIOP ministrada, todos os militares da Guarda têm à disposição, o Manual de Procedimentos SIIOP, colocado na *intranet* da GNR, apresentando-se assim, como um precioso auxiliar de consulta para todos os militares da Guarda, quer seja no primeiro contacto com o sistema, para efeitos de autoformação ou como peça fundamental na reciclagem de conhecimentos adquiridos durante a formação.

A importância da formação e dos Recursos Humanos

Todos os factores são determinantes para o sucesso da implementação e da operacionalização qualitativa e eficiente do SIIOP. Todavia, o factor humano tem, indiscutivelmente, um peso substancial. A operacionalização e exploração do SIIOP exigem uma formação robusta que potencie com especial enfoque o desempenho, a racionalização e a qualidade dos serviços prestados por todos os militares da GNR, sendo premente a sua qualificação em Tecnologias de Informação e Comunicação, sustentada em princípios de qualidade, que se pretendem cada vez mais, baseados na Inovação e no Conhecimento. Nesta óptica e no domínio do SIIOP, é necessário ministrar uma formação especialmente orientada:

- A um atendimento de superior qualidade a ser prestado ao cidadão;
- Identificar e compreender a importância que o SIIOP representa para a reengenharia, inovação organizacional e modernização da GNR, com especial relevo na forma como ele potencia a actividade operacional e como contribui para a Segurança Nacional e Internacional, tendo em consideração as novas dinâmicas criminais globais;
- Apreensão dos novos "Processos de Negócio" que o SIIOP implementa e que, em última análise, agilizam, decisivamente, a prevenção e o combate ao crime e às infracções;
- Transmissão de competências para explorar e manusear o SIIOP com elevados níveis de eficácia e eficiência.

Nos Comandos Territoriais onde o SIIOP está implementado, foi possível ministrar formação *in-loco* aos seus militares. Este tipo de formação é, por experiência adquirida, a única forma viável para garantir um alto nível de qualidade de atendimento ao cidadão e operacionalização eficiente do Sistema. As razões subjacentes são as seguintes:

- Por simular as condições reais e particularidades locais de utilização do SIIOP;
- Dado o grande volume de Recursos Humanos (RH) que vai estar afecto ao SIIOP, ser inviável ministrar-lhes formação de forma centralizada na EG;
- Não ser possível desviar RH, afectos à actividade operacional policial para acções de formação.

Conscientes que as mudanças inerentes à implementação de um sistema desta natureza e dimensão, não são tarefa fácil, antes pelo contrário, exigem um esforço concertado de todos os quadrantes e a necessária Acção de Comando, verifica-se que, embora exista um planeamento de formação e implementação do SIIOP, superiormente definido pelo Comando da Guarda, diversos constrangimentos técnicos e humanos têm provocado atrasos irreversíveis na formação e consequente implementação do sistema.

Outra situação que tem contribuído significativamente, para um notório subaproveitamento dos conhecimentos ministrados durante a formação deve-se ao espaço de tempo que decorre entre a referida formação e a utilização em ambiente real, do sistema, ultrapassando, em alguns casos, os quatro/cinco meses, com os graves prejuízos daí decorrentes que se têm procurado minimizar.

Este factor tem vindo a ser minimizado com a dis-

ponibilização de um perfil adequado em ambiente real e o incentivo da cadeia de comando para que o SIIOP seja utilizado em situações que não implique contacto com o cidadão, situação que tornaria a adaptação mais stressante e transmitiria uma imagem menos positiva no atendimento da GNR, bem como na introdução de expediente mais antigo elaborado antes da formação SIIOP.

Pretende-se que a GNR, com a ajuda do SIIOP e dos seus militares, cresça na qualidade do serviço prestado, chegando cada vez mais perto do cidadão e responda de forma célere e eficaz aos desafios que hoje em dia a sociedade nos coloca.

Pese o facto de não estar concluída a implementação, apesar de se esperar que venha a estar muito em breve, não tenhamos dúvidas de que se trata de um esforço meritório, porque os ganhos associados a este projecto para a Guarda são enormes e irão catapultar verdadeiramente, a GNR para o século XXI.

Sargento-Mor FELICIANO ALVES

BIBLIOGRAFIA

- Decreto Regulamentar n.º 2/95, de 25 de Janeiro de 1995.
- Pela Lei e Pela Grei, Outubro – Dezembro 2010, O SISTEMA INTEGRADO DE INFORMAÇÕES OPERACIONAIS POLICIAIS – SIIOP.
- NEP/GNR - 2.20, de 12 de Dezembro de 2011.

A importância da tecnologia no combate ao crime

A GNR é a força de segurança em Portugal que, sem grandes margens para dúvidas, detém o maior leque de áreas de intervenção[1], claramente definidas no seu decreto orgânico. A salvaguarda de direitos, liberdades e garantias da população no Território Nacional é uma tarefa que carece de elevados níveis de prontidão, capacidade de intervenção e disponibilidade.

Seguindo a abordagem inicial dos níveis de combate ao crime, podemos identificar as várias áreas em que a GNR utiliza as denominadas tecnologias de informação e comunicação. Muitas dessas tecnologias poderão ter mais do que uma utilização. Contudo, as mesmas são um suporte fundamental para a atividade quotidiana dos soldados da lei e da grei.

Na perspetiva da prevenção criminal, podemos referir que a GNR tem investido bastante nesta área (o termo "bastante" terá que ser devidamente adequado ao valor real disponível para investimentos no orçamento anual da GNR, uma vez que mais de 90% desse orçamento é consumido pelas despesas com pessoal). A vertente *"soft tech"* é aquela que tem assistido aos maiores avanços. Esta tendência encontra-se superiormente definida, sendo objeto de recomendações expressas em vários documentos estruturantes da União Europeia, do governo português e, por conseguinte, da própria Guarda.

O desenvolvimento de *"software"* adequado à gestão operacional da GNR, como é o caso do Sistema de Gestão de Ocorrências (SGO), com a integração da georreferenciação[2] dos meios no terreno na mesma plataforma, permite uma maior maximização de meios e, por conseguinte, uma maior eficácia na resposta aos ilícitos criminais.

O mesmo se pode dizer, por exemplo, em relação à utilização de *"hard tech"* nesta vertente do combate ao crime. Os investimentos no Sistema Integrado de Vigilância e Controlo Costeiro, para a vigilância e controlo da costa ou em viaturas descaracterizadas e equipadas com sistema Provida têm contribuído significativamente, para a eficácia global do sistema de prevenção criminal, colaborando para uma resposta integrada mais eficaz na antecipação dos problemas.

Quanto mais eficaz for o sistema de prevenção, menor será o esforço dos sistemas associados de investigação e de repressão criminal, permitindo uma melhor gestão dos meios afetos a estas duas últimas valências.

As demais ferramentas tecnológicas em uso na GNR possibilitam, hoje em dia, uma resposta diferenciada e geradora de um maior sentimento de segurança por parte da população que servimos, além da possibilidade de passar a existir uma normalização e harmonização de procedimentos de trabalho.

É certo que não se consegue quantificar os proveitos de um sistema de prevenção, pois não é possível calcular os lucros gerados pelo mesmo, não se diferenciando o contexto nacional do verificado em estudos realizados noutros países. Contudo, poderemos afirmar que a qualidade da resposta da GNR de hoje é muito superior à verificada há uma década atrás, pese embora as alterações sociais que se têm feito sentir nestes últimos anos.

Por exemplo, ao nível da investigação criminal, uma outra forma de combater o crime, podemos também afirmar que os seus níveis de eficiência são os mais elevados de sempre. Esta posição deve muito à introdução de novas técnicas, à disponibilização de equipamentos tecnológicos e ao constante

[1] Art.º 3.º da Lei n.º 63/2007, de 06 de novembro.
[2] Valência do Sistema Integrado de Redes de Emergência e de Segurança (SIRESP).

acompanhamento da evolução nestas matérias.

A GNR está a conseguir integrar a tecnologia de ponta com a arte e engenho dos seus militares, resultando dessa simbiose um sistema de IC moderno e adaptado às reais necessidades do país. O equipamento hoje disponível para as vertentes da IC está ao nível dos melhores do mundo, possibilitando respostas cada vez mais adequadas para a apresentação dos suspeitos perante a justiça.

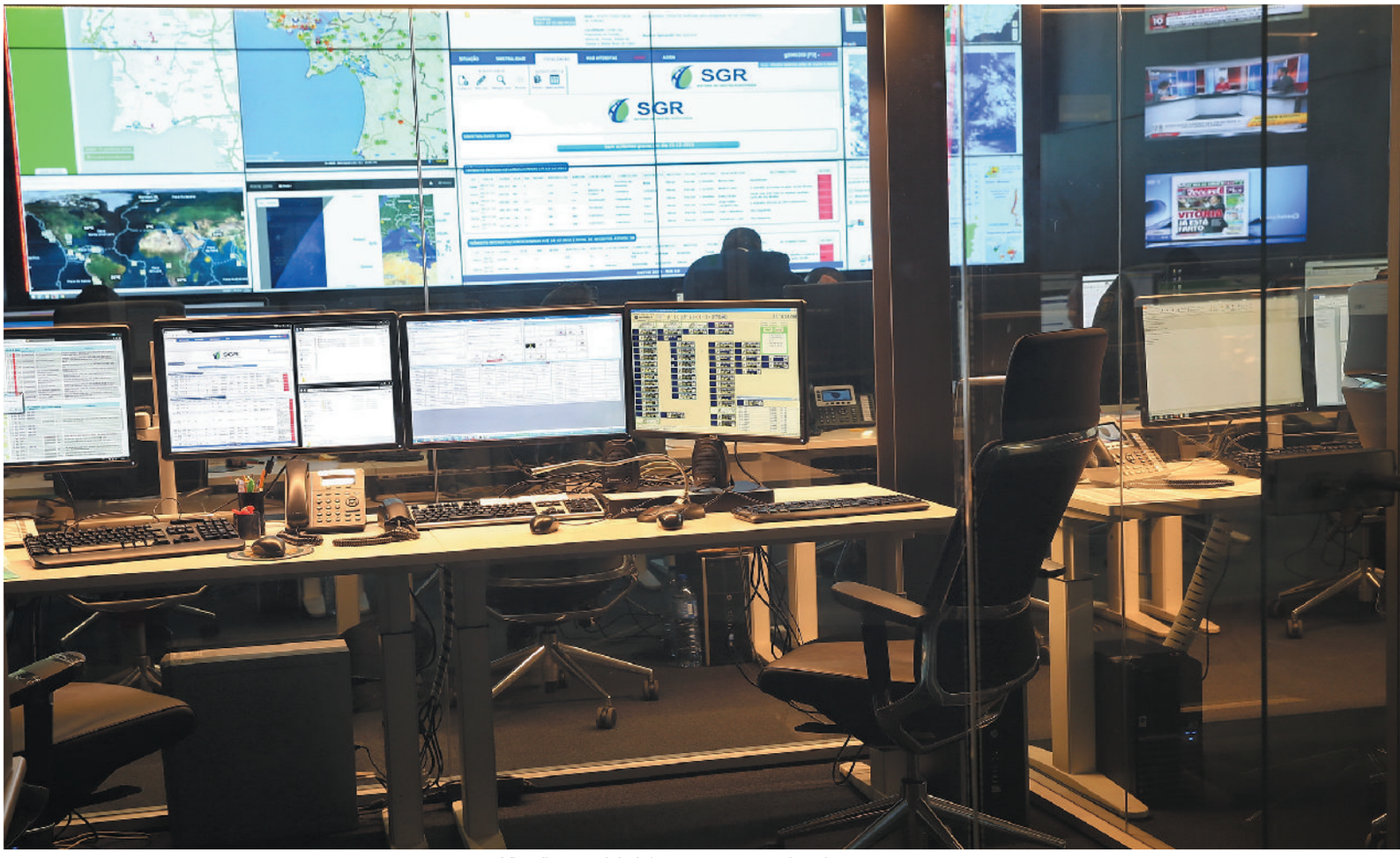
Ao nível dos equipamentos disponíveis para a vertente da repressão criminal existentes na GNR, estão cada vez mais evoluídos e próximos das reais necessidades impostas pelo serviço público que desenvolvemos. Desde *"Remotely Piloted Aircraft Systems"* (RPAS), embarcações de alta qualidade, passando por viaturas blindadas, até ao armamento individual, tudo se tem feito para dotar os militares de tecnologia adequada à árdua missão do dia-a-dia, incrementando os níveis de autoproteção e melhorando a capacidade de atuação.

Não se pode afirmar que a GNR não dispõe da tecnologia necessária para cumprir a missão. Podemos sim dizer que, poder-se-ia melhorar a mesma, por vezes, com um baixo investimento.

Muitas vezes não basta investir em tecnologia. É necessário investir na tecnologia certa. Quando se estuda um sistema de informações policiais, como é o caso do Sistema Integrado de Informações Operacionais de Polícia, não se deve querer desenhar uma máquina que, por si só, consiga movimentar a maior empresa nacional. É necessário ter algumas cautelas. A tecnologia existe para auxiliar o Homem e não para complicar a sua tarefa. O estudo assertivo das necessidades tecnológicas na GNR tem-se desenvolvido de forma transversal, integrada e geradora de valor acrescentado, não apenas para seguir tendências ou modas de cada época. Relembremos, por exemplo, que o sistema *"Long Army Operational System"* (LAOS) esteve operacional durante mais de 20 anos, dando uma resposta cabal às necessidades operacionais, até aos seus últimos dias de vida. E o que é que diferenciava aquele sistema altamente evoluído naquela época, dos existentes atualmente? O mesmo foi desenhado à medida, construído de forma modular e com procedimentos simples, ao invés dos complexos algoritmos que sustentam algumas das bases tecnológicas dos sistemas de informação atuais existentes na GNR, dadas as alterações tecnológicas e socias que hoje se alteram à velocidade de um *click*.

Capitão de Infantaria JOÃO JANEIRO

CCCO – O Projeto



Visualização global da *common operating picture*.

Apostando numa renovada capacidade de comando, controlo e coordenação, assente na modernidade tecnológica, num modelo de policiamento integrado com as outras entidades oficiais baseado em evidências, *evidence lead policing*, e na especialização dos seus recursos humanos nas áreas tecnológicas, a Guarda implementou um novo Centro de Comando e Controlo Operacional (CCCO).

Esta estrutura potencia os recursos operacionais da GNR, reduz os tempos de resposta a incidentes e suporta, de forma tempestiva, o apoio à decisão de toda a atividade operacional da Guarda, tendo em vista a gestão de ocorrências e alocação de meios em conformidade, com base no alinhamento da tecnologia com a Missão da Guarda, proporcionando uma alteração de conceito operacional, a fim de assegurar serviços com maior visibilidade, incrementada qualidade e elevada disponibilidade, junto do cidadão.

A nova estrutura do CCCO visa ainda assegurar a troca de informação operacional em tempo real, garantindo uma imagem única da área de operações, *Common Operating Picture*, tornando mais coerente, eficaz, eficiente e racional, o sistema de informações da Guarda.

O projeto foi conduzido por uma equipa multidisciplinar, integrando membros das diversas Direções do CO, do CCCO, da DIE, DRL, UAG e do Grupo de

Virtual desktop infrastructure que garante a liderança digital da Guarda.

Tecnologias e Sistemas de Informação, envolvendo Oficiais, Sargentos e Guardas, tendo sido coordenado pelo Exmo. General ACO.

Para uma execução e gestão coordenada do projeto do CCCO, houve que efetuar a sua decomposição nas componentes de Infraestruturas, Normativo, Tecnologias e Sistemas de Informação (TSI), Mobiliário e Normativo, com requisitos temporais e especificações técnicas exigentes para cada um dos elementos constituintes.

Como curiosidade tecnológica, na componente TSI foi contemplada uma solução *ultra-thin client* que inclui *storage*, servidores e computação integrada, denominada "*Zero Client*", a qual se caracteriza pela elevada produtividade induzida, poupança energética (decréscimo no consumo em cerca de 97%), redução da pegada ambiental, ausência de armazenamento local assente num ambiente virtual "*virtual desktop infrastructure*", e reduzido espaço de instalação, características que garantem a liderança digital da Guarda nesta área específica.

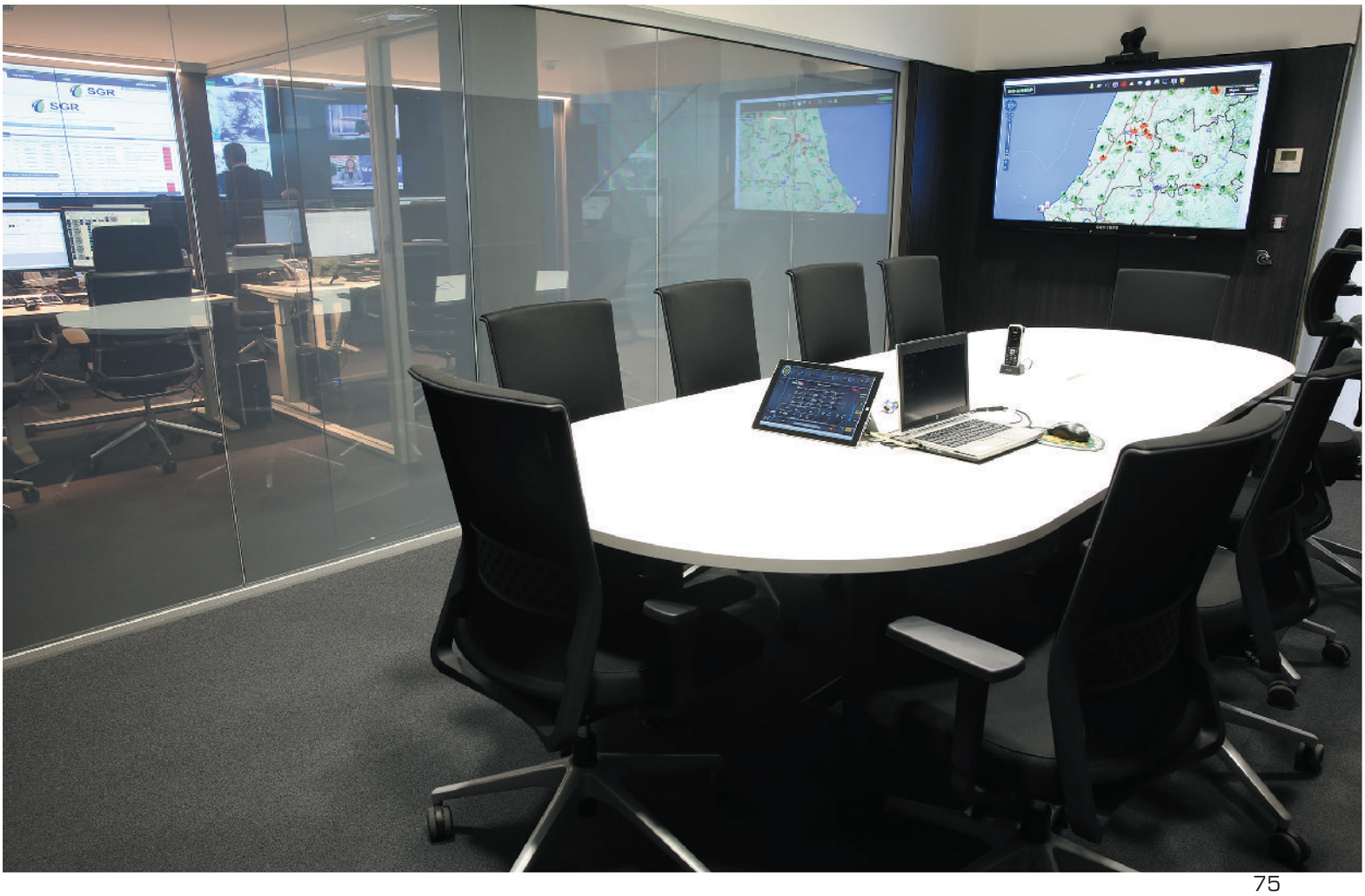
Como solução de visualização global da *common operating picture*, foi implementado um *video wall* baseado em monitores LCD de baixo consumo energético, adequada resolução, de formato normalizado e com natureza comercial que, em caso

de avaria, podem ser facilmente substituídos por outros existentes no mercado, mesmo que de marca diferenciada. O sinal digital pode ser incorporado e distribuído a partir de um servidor acoplado a uma matriz, sendo geridas remotamente as diferentes entradas de vídeo, som e imagem para o *vídeo wall*, projetores e monitores localizados nas diversas salas do CCCO, de forma descentralizada e de acordo com os requisitos de cada utilizador, incluindo sinal digital de televisão.

Foram ainda disponibilizadas nas salas do CCCO, capacidades integradas de videoconferência, ligações para *pressbox* destinadas a conferências de imprensa, sinal vídeo, som e imagem para, e do *video wall*, bem assim como monitores *touch screen* destinados a iluminar situações tático-policiais.

O projeto teve uma duração aproximada de seis meses, desde o início das obras na infraestrutura do antigo auditório do Comando-Geral até à sua inauguração oficiosa, continuando a ser desenvolvidas ações de adaptação e beneficiação das instalações, melhoria contínua dos processos, integração e interoperabilidade dos sistemas de informação.

Pelo Coronel ART ENGGEO, LUÍS NUNES



Capacidades integradas de videoconferência, *pressbox*, som, vídeo e iluminação de situações tático-policiais.