SGMAI
SECRETARIA GERAL
MINISTÉRIO DA ADMINISTRAÇÃO INTERNA

PROCEDIMENTO N.º 128/DSUMC/17

Aquisição de Software OSINT (Open Source Intelligence),

Licenciamento e assistência técnica

Centro de Informações GNR

CADERNO DE ENCARGOS

PARTE I

Cláusula 1.ª

Objeto

1. O presente caderno de encargos tem por objeto a aquisição de Software OSINT (Open Source Intelligence), respetivo licenciamento, equipamentos de suporte, serviços de manutenção e assistência técnica durante 2 (dois) anos, para o Centro de Informações OSINT da GNR.
2. As características e especificações constam das Especificações Técnicas descritas na Parte II deste Caderno de Encargos.

Cláusula 2.ª

Disposições por que se rege a prestação dos serviços

1. O fornecimento do bem objeto do presente contrato obedece:
    a) Às cláusulas do Contrato e ao estabelecido em todos os elementos e documentos que dele fazem parte integrante;
    b) Ao Código dos Contratos Públicos, doravante designado "CCP".
2. Para efeitos do disposto na alínea a) do número anterior, consideram-se integrados no Contrato, sem prejuízo do disposto no nº 4 do artigo 96º do CCP:
    a) O clausulado contratual, incluindo os ajustamentos propostos de acordo com o disposto no artigo 99.º do CCP e aceites pela entidade adjudicante nos termos do disposto no artigo 101.º desse mesmo Código;
    b) Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que tais erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do disposto no artigo 61.º do CCP;
    c) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
    d) O Caderno de Encargos;
    e) A proposta adjudicada;
    f) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário;
    g) Todos os outros documentos que sejam referidos no clausulado contratual ou no Caderno de Encargos.

Cláusula 3.ª

Preço base e contratual

1. O preço base, máximo que a entidade adjudicante se dispõe a pagar pelo fornecimento de bens e prestação de serviços objeto do presente procedimento é **275.000,00€** (duzentos e setenta e cinco mil euros), valor ao qual acresce o IVA à taxa legal em vigor.
2. Consideram-se incluídos no preço, todas as despesas que o adjudicatário tenha de realizar com a entrega dos bens, incluindo todas as despesas com a instalação, transporte, deslocações, meios humanos, técnicos e equipamentos, constantes do caderno de encargos.

Cláusula 4.ª

Prazo e local de entrega

1. O prazo máximo para entrega, instalação e configuração do software, é de 30 (trinta) dias úteis, após a receção da nota de encomenda, a emitir pela DRL - Direção de Recursos Logísticos da Guarda Nacional Republicana;

2. Os bens deverão ser entregues, instalados e configurados nos Centros de Dados da entidade adjudicante, sito no Comando Geral da GNR, no Largo do Carmo, 1200-092 Lisboa.

Cláusula 5.ª

Condições e prazo de pagamento

1. O pagamento do encargo global do presente contrato será efetuado numa única prestação, após a receção definitiva dos bens e contra a entrega da respetiva fatura.
2. O pagamento será efetuado por transferência bancária no prazo máximo de 30 dias após a receção da nota de encomenda, a emitir pela DRL - Direção de Recursos Logísticos da Guarda Nacional Republicana.
3. Pelo atraso no cumprimento de qualquer obrigação pecuniária, a entidade adjudicante fica obrigada ao pagamento de juros de mora, nos termos da Lei n.º 3/2010 de 27 de abril.
4. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicado nas fatura, deve esta comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

Cláusula 6.ª

Obrigações principais do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o adjudicatário as seguintes obrigações principais:

a) Obrigação de fornecer os bens e os serviços de instalação e garantia técnica tendo em consideração o presente Caderno de Encargos e as necessidades da entidade adjudicante;
b) Obrigação de substituição dos bens/serviços rejeitados, em igual período proposto para a entrega daquele bem ou prestação daquele serviço, contados a partir da data da emissão da notificação do facto.
c) Obrigação de prestar a formação on-job necessária ao correto manuseamento e cabal aproveitamento do sistema.

2. Cabe ainda ao adjudicatário a responsabilidade:
   a) Do licenciamento do software e definição da arquitetura de serviços;
   b) A instalação do harware e da plataforma;
   c) A configuração base da plataforma;
   d) A instalação e configuração de fontes/motores/integrações específicas;
   e) A Manutenção e atualização da plataforma;
   f) A Gestão de incidentes de funcionamento da plataforma.
3. Devendo o adjudicatário apoiar a entidade adjudicante:
   a) Na investigação em blackmarkets;
   b) No roubo de identidade, privacidade, compliance;
   c) Na formação em fontes abertas (OSINT);
   d) No hacktivismo, terrorismo, crime organizado;
   e) No cibercrime.

4. O título acessório, o adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 7.ª

Conformidade e operacionalidade bens

1. O adjudicatário obriga-se a entregar, instalar e configurar os bens objeto do contrato de acordo com as caraterísticas, especificações e requisitos técnicos previstos na Parte II – Especificações Técnicas do presente Caderno de Encargos.
2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam.

3. O adjudicatário é responsável perante a entidade adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 8.ª

Inspeção e testes

1. Efetuada entrega, instalação e configuração do bem objeto do presente procedimento, a entidade adjudicante, por si ou através de terceiro por ela designado, procede, no prazo de 5 (cinco) dias, à inspeção qualitativa do mesmo, com vista a verificar, respetivamente, se os mesmos correspondem às caraterísticas, especificações e requisitos técnicos definidos na Parte II – Especificações Técnicas do presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. Durante a fase realização de testes, o adjudicatário deve prestar à entidade adjudicante toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito.
3. Os encargos com a realização dos testes, devidamente comprovados, são da responsabilidade do adjudicatário.

Cláusula 9.ª

Defeitos ou discrepâncias

1. No caso de os testes previstos na cláusula anterior não comprovarem a conformidade do bem com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as caraterísticas, especificações e requisitos técnicos definidos na Parte II – Especificações Técnicas do presente Caderno de Encargos, a entidade adjudicante deve de isso informar, por escrito, o adjudicatário.
2. No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa e no prazo razoável que for determinado pela entidade adjudicante, às reparações ou substituições necessárias para garantir o cumprimento das exigências legais e das caraterísticas, especificações e requisitos técnicos exigidos.
3. Após a realização das reparações ou substituições necessárias pelo adjudicatário, no prazo respetivo, a entidade adjudicante procede à realização de novos testes de aceitação, nos termos da cláusula anterior.

Cláusula 10.ª

Aceitação definitiva dos bens

1. Caso os testes a que se refere a Cláusula 8.ª comprovem a conformidade do bem e da respetiva instalação com as exigências legais e neles não sejam detetados quaisquer defeitos ou discrepâncias

com as características, especificações e requisitos técnicos definidos na Parte II – Especificações Técnicas do presente Caderno de Encargos, no prazo máximo de 5 (cinco) dias a contar do final dos testes, considera-se feita a aceitação definitiva dos bens.

2. Com a aceitação definitiva dos bens, ocorre a transferência da posse e da propriedade do bem objeto do presente contrato para a entidade adjudicante, bem como do risco de deterioração ou perecimento do mesmo, sem prejuízo das obrigações de garantia que impendem sobre o adjudicatário.
3. A aceitação definitiva a que se refere o n.º 1 não implica a aceitação de eventuais defeitos ou de discrepâncias dos referidos bem objeto do presente contrato, com as exigências legais ou com as caraterísticas, especificações e requisitos técnicos previstos na Parte II – Especificações Técnicas do presente Caderno de Encargos.

Cláusula 11.ª

Garantia

O prazo de garantia do licenciamento e dos serviços de manutenção e assistência técnica não deve ser inferior a 24 meses, e será contado a partir da receção dos mesmos.

Cláusula 12.ª

Níveis dos serviços

As atividades de manutenção e assistência técnica têm a necessidade de ser garantidas através de um tempo máximo de intervenção (SLA – Service Level Agreement) para os casos de avarias ou erros do software ou de desconfiguração do sistema com **tempos de resolução até ao dia útil seguinte** (Next Business Day).

Cláusula 13.ª

Penalidades

1. Em caso de incumprimento injustificado das obrigações contratuais por parte do adjudicatário, poderá a entidade adjudicante aplicar as sanções contratuais até ao limite de 20% do preço contratual.
2. No caso de incumprimento do prazo fixado para a entrega, instalação e configuração dos bens nos termos do n.º 1 da Cláusula 4.ª do presente Caderno de Encargos, poderá a entidade adjudicante aplicar as seguintes penalidades:

Atraso	Penalidade
Até ao 5.º dia	0,05 % do valor contratual, por cada dia de atraso
A partir do 6.º dia	0,1 % do valor contratual , por cada dia de atraso

3. No caso de atraso no cumprimento dos tempos de resposta previstos na Cláusula 12.º do presente caderno de encargos, poderá a entidade adjudicante aplicar as seguintes penalidades contratuais:

Atraso	Penalidade
Até ao 2.º dia útil seguinte	0,05 % do valor contratual, por cada hora de atraso
A partir da 3.º dia útil seguinte	0,1 % do valor contratual , por cada hora de atraso

4. Se for atingido o limite previsto no número 1. e a entidade adjudicante decidir não proceder à resolução do contrato por dela resultar grave dano para o interesse público, aquele limite é elevado para 30% do valor do preço contratual.
5. Caso se verifique a aplicação das penalidades previstas no n.º 2 do artigo anterior, será descontado ao pagamento a efetuar pela entidade adjudicante ao adjudicatário.
6. As sanções pecuniárias previstas no n.º 3 são deduzidas ao valor da caução.

Cláusula 14.ª

Execução e libertação da caução

1. A caução prestada pelo adjudicatário pode ser executada pela entidade adjudicante, sem necessidade de prévia decisão judicial ou arbitral, para satisfação de quaisquer importâncias que se mostrem devidas por força do não cumprimento por aquele das obrigações legais ou contratuais, designadamente as seguintes:
   a) Sanções pecuniárias aplicadas nos termos previstos no contrato;
   b) Prejuízos incorridos pela entidade adjudicante, por força do incumprimento do contrato;
   c) Importâncias fixadas no contrato a título de cláusulas penais.
2. A execução parcial ou total de caução prestada pelo adjudicatário implica a renovação do respetivo valor, no prazo de 15 dias após a notificação pela entidade adjudicante para esse efeito.
3. A liberação da caução ocorre nos termos do definido no n.º4 do artigo 295.º do Código dos Contratos Públicos.

Cláusula 15.ª

Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, designadamente greves ou outros conflitos coletivos de trabalho, for impedido de cumprir as obrigações assumidas no contrato.

2. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 16.ª

Sigilo

O adjudicatário obriga-se a guardar sigilo de todas as informações que obtiver no âmbito da execução do Contrato relativamente à entidade adjudicante e ao objeto da prestação de serviços.

Cláusula 17.ª

Cessão de posição contratual e subcontratação

1. O adjudicatário poderá ceder a posição contratual ou subcontratar mediante prévia autorização da entidade adjudicante.
2. Para efeitos da autorização prevista no número anterior, deve o adjudicatário apresentar uma proposta fundamentada, instruída com todos os documentos de habilitação relativos ao cessionário ou ao subcontratado, que foram exigidos ao adjudicatário no presente procedimento.

Cláusula 18.ª

Deveres de informação

1. As partes estão vinculadas pelo dever de colaboração mútua, designadamente no tocante à prestação recíproca de informações necessárias à boa execução do contrato, sem prejuízo dos deveres de informação previstos no artigo 290º do CCP.
2. Em especial, cada uma das partes deve avisar de imediato a outra de quaisquer circunstâncias, constituam ou não força maior, que previsivelmente impeçam o cumprimento ou o cumprimento tempestivo de qualquer uma das suas obrigações.
3. No prazo de dez dias após a ocorrência de tal impedimento, a parte deve informar a outra do tempo ou da medida em que previsivelmente será afetada a execução do Contrato.

Cláusula 19.ª

Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do CCP, para o domicílio ou sede contratual de cada uma, identificados no *Contrato*.

2. Qualquer alteração das informações de contacto constantes do *Contrato* deve ser comunicada à outra parte.

Cláusula 20.ª

Resolução do contrato

1. Para além das situações previstas no nº 1 do artigo 333º e nos artigos 334º e 335º do CCP, a entidade adjudicante pode resolver o contrato quando os serviços não sejam prestados por cinco dias seguidos ou dez dias interpolados e o adjudicatário não apresente justificação para esse facto.
2. O disposto no número anterior não prejudica o direito de indemnização nos termos gerais, nomeadamente pelos prejuízos decorrentes da adoção de novo procedimento de formação de contrato.
3. Nos casos previstos no número anterior, havendo lugar a responsabilidade do adjudicatário, será o montante respetivo deduzido das quantias devidas, sem prejuízo da entidade adjudicante poder executar as garantias prestadas pelo fornecedor.

Cláusula 21.ª

Foro competente

Para resolução de todos os litígios decorrentes do Contrato fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

PARTE II - ESPECIFICAÇÕES TÉCNICAS

1. ENQUADRAMENTO

a. A estratégia nacional de prevenção e combate ao crime centra-se na disponibilidade dos meios, materiais tecnológicos, que permitam habilitar as autoridades competentes a fazer face aos desafios e ameaças cada vez mais complexas.

b. No âmbito da Estratégia da Guarda 2020 foi identificado e definido enquanto objetivo estruturante a edificação de um Sistema de Informações com vista à prevenção da criminalidade, tendo sido criado o Centro de Informações/OSINT, que visa a permanente monitorização, acompanhamento, análise e disseminação de informações policiais e criminais em apoio das atividades e operações correntes e futuras, auxiliando no processo de tomada de decisão mas, cuja implementação, requer a aquisição de um conjunto de software, que satisfaça as necessidades operacionais dessa estrutura.

c. Assim, está associada a necessidade de criar uma estrutura na Guarda, destinada à pesquisa, recolha e tratamento de informações provenientes de fontes abertas que possibilitem organizar e auxiliar o processo de tomada de decisão, cuja implementação, requer a aquisição de um conjunto de software, que satisfaçam as necessidades operacionais dessa estrutura.

d. Face ao acima referido, torna-se necessário dotar a GNR de uma capacidade tecnológica que permita adquirir valências ao nível da recolha de informação e da estruturação e análise de dados, devendo ser assegurada:

   (1) Ao nível da recolha e tratamento de dados:

      a. Permitir a integração de quantidades massivas de dados;

      b. Recolher e integrar informação do tipo não estruturado (documentos, vídeo e imagem) a partir da internet (e.g. através de *crawlers* de dados);

      c. Estar capacitado a detetar o idioma de origem dos dados, identificando possíveis jargões ou calões;

      d. Gerar alarmísticas, monitorizando alterações ou evoluções relacionadas com determinada rede, evento, *ciberpersona* ou utilizador real;

      e. Deter a capacidade de recolher e analisar dados na *deepweb*.

   (2) Ao nível da estruturação/análise de informação:

      a. Monitorizar em "*real-time*" atividades de índole delituosa, criminal ou hostil;

      b. Permitir a indexação de informação não estruturada relacionando o seu conteúdo por temáticas e entidades;

c. Deter ferramentas de pesquisa, monitorização, de análise de dados e de documentos;
d. Deter ferramentas amigáveis de representação gráfica de incidentes, eventos, entidades e das suas relações, gerando estruturas gráficas de fácil leitura, estabelecendo relações entre redes e indivíduos, objetos, entidades e locais possibilitando uma melhor interpretação e compreensão do(s) centro(s) de gravidade/influência;
e. Permitir a recolha e a integração de dados originários de diferentes fontes de informação;
f. Permitir efetuar consultas gerais à informação através de pesquisas unificadas a partir de todos os repositórios de dados ligados ao sistema;
g. Deter capacidade de se integrar a sistemas de informação geográfica, permitindo efetuar a geolocalização e o geoprocessamento dos seus dados;
h. Deter ferramentas de identificação e monitorização de temáticas ou expressões de interesse no ciberespaço (e.g. *sites*, *blogs*, fora, *chats*, etc) recorrentes ou pré-definidas, identificando e acompanhando as atividades de *ciberpersonas* ou utilizadores reais de interesse;
i. Identificar e analisar de forma automática relações entre pessoas, grupos, sites, domínios, redes e afiliações com serviços online, gerando grafos de relações e de influência;
j. Dispor de ferramentas para apoio a analistas de informação;
k. Dispor de ferramentas de análise estatística e predição de eventos.

(3) Ao nível dos email's:
a. Recolher e efetuar a análise do cabeçalho técnico de um email;
b. Identificar possíveis *usernames* que podem estar associados ao email e o seu utilizador real;
c. Efetuar o rastreamento do seu percurso desde o seu emissor;
d. Identificar as referências de um determinado email ou conjunto de emails no ciberespaço (e.g. redes sociais, sites, *blogs*, fora, etc);
e. Georreferenciar a sua origem.

(4) Ao nível da web e das redes sociais:
a. Predizer ações planeadas por grupos *hacktivistas*, através da monitorização das suas atividades online;
b. Monitorizar em "real-time" as atividades dos grupos de *hacktivismo*, os seus movimentos e ações;

c. Analisar as atividades dos grupos de *hacktivistas* que operem na internet, detetando as suas ligações com contas suspeitas;
d. Efetuar a análise semântica de dados em linguagem natural (e.g. *Natural Processing Language* – NPP) e de calão/jargões entre utilizadores e comunidades, "*posts*" (texto, imagem, vídeo) e atividades nas redes sociais e outros canais de comunicação web;
e. Efetuar o "*Sentiment-analysis*" relativo a tópicos de discussão, de interesse ou os relativos a determinada entidade(s);
f. Georreferenciar atividades e "*posts*" relativas a *ciberpersonas* a partir das redes sociais;
g. Monitorizar e detetar em tempo real, através da recolha de elevadas quantidades de informação em fontes abertas como a *deep* e *dark-web*, atividades ilegais pela inserção de dados como número de cartões de crédito, números de conta, documentos falsificados, etc.

(5) Outras valências:
a. Permitir efetuar um "*Police Case Management*", fazendo o registo sucessivo dos acontecimentos;
b. Interoperar com o software de análise i2 e os SIGAOp internos e outros sistemas de informação externos;
c. Garantir uma fácil visualização e compreensão do fenómeno em causa, permitindo um fácil desmontar de processos;
d. Permitir reunir, apresentar, cruzar e analisar dados por meio de diagramas/grafos;
e. Possibilitar a criação de base de dados multi-utilizador, possibilitando o trabalho em equipa ou individualmente.

e. Ao dotar a GNR com esta capacidade tecnológica, contribui-se para a implementação dos Objetivos Operacionais n.º3 (OOp 03) e n.º4 (OOp 04) do Plano Estratégico da Guarda 2020, nomeadamente potenciar o sistema de informações da Guarda e potenciar o processo de produção de informações, respetivamente. O OOp 03 traduz-se nos indicadores 001 e 002, cujas principais ações são a implementação do sistema de informações da Guarda, a orientação do patrulhamento pelas informações (Intelligence led policing) e a predição do crime. Quanto ao OOp 04, traduz-se no indicador I001 cujas principais ações passam pela elaboração de relatórios de notícias, relatórios OSINT e relatórios de informações.
f. A satisfação desta necessidade da Guarda permite:

(1) Consolidar a qualidade da ação policial no âmbito da atividade de investigação criminal;
(2) Aumentar a capacidade para desenvolver ações de prevenção, de deteção e de investigação de crimes;
(3) Aumentar a capacidade de recolha e análise de informações, para melhorar a eficácia da prevenção e combate aos fenómenos criminais, terrorismo e criminalidade transfronteiriça;
(4) Assegurar 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;
(5) Proceder à pesquisa, recolha e tratamento de informações de fontes abertas, antecipando e identificando atempadamente ameaças emergentes, prevenindo e monitorizando atividade criminais relevantes ou socialmente divergentes;
(6) Possibilitar o desenvolvimento de um policiamento orientado pelas informações;
(7) Manter informado e atualizado o Comando Operacional da Guarda sobre qualquer notícia, informação, evento ou atividade pertinente para o desenvolvimento da missão da Guarda.
(8) A solução deve ser “on-promise”.

2. GENERALIDADES

a. No âmbito da Estratégia da Guarda 2020 foi identificado e definido enquanto objetivo estruturante a edificação de um Sistema de Informações com vista à prevenção da criminalidade, tendo sido criado o Centro de Informações/OSINT (Open Source Intelligence).

b. Torna-se necessário dotar a GNR de uma capacidade tecnológica que permita elevadas valências ao nível da recolha de informação e da estruturação e análise de dados, devendo:

(1) Permitir uma recolha de dados, de forma automatizada, tanto de um grande volume de dados residente em bases de dados internas, como externas, como de variadas fontes abertas (OSINT), onde se inclui redes sociais, sites, blogs, chats, entre outros;

(2) Permitir a estruturação/análise de informação, ao nível dos email’s;

(3) Analisar, classificar e organizar a informação recolhida, produzindo inteligência de suporte a tomadas de decisão;

(4) Interoperar com o *software* de análise i2 e com os Sistemas de Informação de Gestão Operacional (SIGAOp) da Guarda;

(5) Permitir a criação de modelos de conhecimento para utilização futura com os dados recolhidos;

(6) Permitir correlacionar dados e criar informações relevantes através de relatórios e gráficos;

(7) Identificar modelos e padrões de dados;

(8) Auxiliar a tomada de decisão mais rápida e eficiente através de uma capacidade de análise de tendências e identificação de ameaças e oportunidades;

(9) Utilizar sistemas de alerta e de rastreamento, notificação de mudanças significativas ou atualizações em massa em fontes de informação.

3. REQUISITOS TÉCNICOS MINIMOS

a. Pretende-se assegurar a aquisição, a instalação, a manutenção do licenciamento e do equipamentos de suporte, bem como a respetiva assistência técnica durante 2 anos de um software informático capaz de fornecer ao utilizador da GNR, informação de análise respeitante a grande volume de dados, de forma estruturada, devendo ter como **requisitos técnicos mínimos** os seguintes:

(1) Deve ser focado no utilizador humano. O utilizador humano terá de tomar a decisão final e é o próprio que decide se a informação final é válida ou se padece de redefinição dos objetivos com vista a obter informação adicional.

(2) Permitir a criação de conectores específicos para a recolha de informação automática, no mínimo, nas seguintes fontes:

(a) Bases de dados internas e externas à GNR (ligação direta).

(b) Motores de pesquisa:

- Google;
- Bing;

- Yahoo;
- Google Scholar;
- SHODAN

(c) Redes Sociais:

- Twitter;
- Facebook;
- Google Plus;
- Youtube;
- Instagram.

(d) Notícias:

- Crawlers;
- RSS;
- Teletipos.

(e) Sistemas:

- Email;
- Unidades de Rede

(f) Alertas do Google

(g) Outros:

- Wordpress;
- Dropbox;
- Paste (Pastebin e sites análogos);
- IRC;
- Github;
- Zone-H.

(3) Permitir fazer pesquisas a várias fontes na *deep* e *dark web* sem exposição;

(4) Permitir a inclusão customizada de outras fontes tais como outros motores de pesquisa, e outras redes sociais, entre outros, não identificados acima em 2.a.(2);

(5) Permitir a integração, não só com outras fontes de dados, mas também com outras plataformas de investigação, nomeadamente com o IBM i2 Analyst Notebook;

(6) Permitir a criação de unidades orgânicas (instâncias a serem utilizadas entre diferentes grupos ou unidades da GNR), e que podem, ou não, partilhar informação entre si;

(7) Ter um interface com o utilizador (GUI) com capacidade de apresentação multi-idioma, encontrando-se disponível o idioma português, entre outros configuráveis;

(8) Ter incluído um serviço de anonimização, com as seguintes características mínimas:

I. Possibilidade de ligação a proxy com 1 Gbps de conetividade sem restrições;

II. Possibilidade gerir 10 IPs estáticos (round-robin).

(9) Garantir o fornecimento e instalação de uma arquitetura de hardware de suporte ao software OSINT em aquisição, suportada no mínimo em dois servidores, em que cada um deve ter no mínimo as seguintes caraterísticas:

I. 2 CPU Standard (família Intel XEON E5-2650 v4 2.2GHz ou equivalente).

II. 32GB de memória RAM.

III. Discos:

- 2 HD 600 GB 15K RPM SAS.
- 4 HD 1.8 TB 10K RPM SAS.

IV. Sistema operativo incluído.