Bando DIS 2026. Cyber, OSINT ed ecofin: i profili degli 007 italiani

Maria Cattini | 19/02/2026 | Open source intelligence

Altro che trench e microspie. Nel 2026 l'intelligence italiana cerca analisti di dati, esperti di crittografia, specialisti OSINT e profili economico-finanziari capaci di leggere i mercati prima che diventino una crisi.

Il nuovo avviso pubblico del Sistema di informazione per la sicurezza della Repubblica segna un cambio netto di linguaggio.
La parola chiave non è "operazione". È competenza.

La scadenza è chiara: candidature entro il 20 marzo 2026.
E il messaggio è altrettanto diretto: la sicurezza nazionale oggi passa dal calcolo ad alte prestazioni, dal deep web e dai flussi finanziari globali.

Cosa prevede il bando DIS 2026

L'iniziativa è coordinata dal Dipartimento delle Informazioni per la Sicurezza (DIS) e rientra nella cornice normativa definita dalla legge 124 del 3 agosto 2007, che ha riformato l'architettura dell'intelligence italiana.

Lo slogan scelto è semplice: "Il tuo talento al servizio dell'Italia". Le candidature si presentano online, tramite il portale istituzionale, con credenziali digitali come SPID o CIE .

Ma il cuore dell'avviso non è la procedura. È l'elenco delle competenze richieste.

Area tecnologica: supercalcolo, AI e OSINT

High Performance Computing e calcolo avanzato

Il primo blocco riguarda il dominio tecnologico. Si cercano profili capaci di gestire architetture complesse, cluster di calcolo, codice parallelo e ottimizzazione delle prestazioni.

Non si tratta di mansioni teoriche. Parliamo di ambienti dove l'analisi deve essere rapida, scalabile, verificabile.

Quando un'amministrazione pubblica chiede competenze tipiche di centri di ricerca o aziende di cybersecurity, il segnale è evidente: la frontiera della sicurezza è diventata computazionale.

OSINT, deep web e dark web

Il bando menziona in modo esplicito attività di ricerca, raccolta e analisi di dati da fonti aperte, inclusi i livelli più complessi del web.

Qui entra in gioco la parola chiave che molti cercano online: OSINT.

Che significa OSINT?
Open Source Intelligence. Analisi strutturata di dati pubblicamente accessibili: social network, registri societari, forum, archivi, metadati, immagini satellitari.

Non è hacking. È metodo.

Il passaggio rilevante è questo: l'intelligence non punta solo al "segreto", ma alla capacità di distinguere segnali utili dal rumore informativo. In un ecosistema dominato da propaganda, manipolazione e sovraccarico di dati, la competenza analitica vale più della quantità.

Area economico-finanziaria: proteggere i mercati

Ecofin e tutela del patrimonio industriale

Un secondo blocco riguarda laureati in discipline economiche.
Obiettivo: analizzare mercati finanziari, titoli di Stato, dinamiche creditizie e minacce al know-how tecnologico nazionale.

Il riferimento non è casuale. Le scalate ostili, le filiere opache e la fuga di tecnologia rappresentano oggi leve strategiche nelle competizioni geopolitiche.

Chi lavora in ecofin nell'intelligence non fa solo analisi contabile. Collega dati finanziari, relazioni societarie e interessi transnazionali.

Evasione, elusione e flussi opachi

Il bando richiama anche la capacità di leggere forme complesse di evasione ed elusione fiscale . Qui l'OSINT si intreccia con l'analisi finanziaria. Banche dati pubbliche, visure, registri internazionali, leak strutturati: tutto può diventare materia prima per ricostruire reti economiche.

Profili per diplomati: cyber e analisi operativa

Non solo laureati. Una parte della selezione è aperta a diplomati con competenze cyber e capacità di analisi di fonti aperte.

Il messaggio è chiaro: la pipeline formativa conta, ma conta anche la competenza reale.

Chi ha esperienza in:

• raccolta strutturata di dati online
• monitoraggio del deep web
• analisi di segnali digitali

può trovare uno spazio, se dimostra metodo e rigore. Il contesto europeo parla di carenza di competenze digitali avanzate. Il report ENISA evidenzia una domanda crescente nel settore cybersecurity e un gap ancora significativo tra offerta e fabbisogno.

In Italia, l'Osservatorio sulle Competenze Digitali 2025 segnala centinaia di migliaia di profili ICT mancanti.

La competizione non è solo tra Stati. È tra settore pubblico e grandi multinazionali tech.
L'intelligence, per attrarre talenti, deve competere su motivazione, missione e prospettiva strategica.

Come candidarsi: passaggi operativi

1. Accesso al portale

Le candidature si presentano online nella sezione “Lavora con noi” del portale istituzionale.

Sono richieste credenziali digitali. Senza SPID o CIE, l’invio non è completabile.

2. Scadenza

Il termine è fissato alle ore 24:00 del 20 marzo 2026. Oltre quella data, la procedura si chiude.

3. Candidatura spontanea

Il DIS ricorda che resta possibile inviare candidature spontanee anche al di fuori dell’avviso mirato.

I settori citati si estendono a tecnologie dual use, sistemi satellitari, telerilevamento, lingue rare, produzione grafica e infografica.

La sicurezza nazionale è un campo ibrido. Dal codice alla geopolitica, dalle immagini satellitari ai flussi finanziari.

Pro e contro di lavorare nell’intelligence digitale

Vantaggi

Impatto strategico reale.
Accesso a contesti ad alta complessità.
Possibilità di lavorare su minacce concrete, non su simulazioni accademiche.

Criticità

Elevato livello di responsabilità.
Riservatezza stringente.
Percorsi professionali meno visibili rispetto al settore privato.

Non è una carriera glamour.
È una carriera ad alta pressione.

OSINT e sicurezza nazionale: cosa cambia

Molti cercano online: “OSINT è legale?”
Sì, se si basa su fonti pubbliche e su metodologie corrette.

La differenza sta nel metodo.
Raccogliere dati non basta. Serve verificarli, contestualizzarli, incrociarli.

Nel 2026 l’intelligence italiana manda un messaggio chiaro:
non basta avere accesso ai dati. Bisogna saperli interpretare.

https://coondivido.it/entrare-servizi-segreti-italiani/

Un segnale al mercato del lavoro

Il **Bando DIS 2026** racconta qualcosa di più di una semplice selezione.

Racconta un Paese che riconosce la centralità di:

- cybersicurezza
- open source intelligence
- analisi economico-finanziaria

• supercalcolo e intelligenza artificiale

Chi oggi studia cybersecurity, data science o OSINT si trova davanti a una domanda concreta. Non teorica.

La domanda è: vuoi mettere le tue competenze al servizio della sicurezza nazionale?

Vuoi approfondire come funziona davvero l'OSINT e quali competenze servono per lavorare tra cyber e intelligence?
Iscriviti alla newsletter OSINT & AI per Tutti su https://coondivido.substack.com/
Unisciti anche ai nostri canali Telegram:
https://t.me/osintaipertutti
https://t.me/osintprojectgroup
Altro che trench e microspie. Nel 2026 l'intelligence italiana cerca analisti di dati, esperti di crittografia, specialisti OSINT e profili economico-finanziari capaci di leggere i mercati prima che diventino una crisi.

Il nuovo avviso pubblico del Sistema di informazione per la sicurezza della Repubblica segna un cambio netto di linguaggio.
La parola chiave non è "operazione". È competenza.

La scadenza è chiara: candidature entro il 20 marzo 2026.
E il messaggio è altrettanto diretto: la sicurezza nazionale oggi passa dal calcolo ad alte prestazioni, dal deep web e dai flussi finanziari globali.

Cosa prevede il bando DIS 2026

L'iniziativa è coordinata dal Dipartimento delle Informazioni per la Sicurezza (DIS) e rientra nella cornice normativa definita dalla legge 124 del 3 agosto 2007, che ha riformato l'architettura dell'intelligence italiana.

Lo slogan scelto è semplice: "Il tuo talento al servizio dell'Italia". Le candidature si presentano online, tramite il portale istituzionale, con credenziali digitali come SPID o CIE .

Ma il cuore dell'avviso non è la procedura. È l'elenco delle competenze richieste.

Area tecnologica: supercalcolo, AI e OSINT

High Performance Computing e calcolo avanzato

Il primo blocco riguarda il dominio tecnologico. Si cercano profili capaci di gestire architetture complesse, cluster di calcolo, codice parallelo e ottimizzazione delle prestazioni.

Non si tratta di mansioni teoriche. Parliamo di ambienti dove l'analisi deve essere rapida, scalabile, verificabile.

Quando un'amministrazione pubblica chiede competenze tipiche di centri di ricerca o aziende di cybersecurity, il segnale è evidente: la frontiera della sicurezza è diventata computazionale.

OSINT, deep web e dark web

Il bando menziona in modo esplicito attività di ricerca, raccolta e analisi di dati da fonti aperte, inclusi i livelli più complessi del web.

Qui entra in gioco la parola chiave che molti cercano online: OSINT.

Che significa OSINT?
Open Source Intelligence. Analisi strutturata di dati pubblicamente accessibili: social network, registri

societari, forum, archivi, metadati, immagini satellitari.

Non è hacking. È metodo.

Il passaggio rilevante è questo: l'intelligence non punta solo al "segreto", ma alla capacità di distinguere segnali utili dal rumore informativo. In un ecosistema dominato da propaganda, manipolazione e sovraccarico di dati, la competenza analitica vale più della quantità.

Area economico-finanziaria: proteggere i mercati

Ecofin e tutela del patrimonio industriale

Un secondo blocco riguarda laureati in discipline economiche.
Obiettivo: analizzare mercati finanziari, titoli di Stato, dinamiche creditizie e minacce al know-how tecnologico nazionale.

Il riferimento non è casuale. Le scalate ostili, le filiere opache e la fuga di tecnologia rappresentano oggi leve strategiche nelle competizioni geopolitiche.

Chi lavora in ecofin nell'intelligence non fa solo analisi contabile. Collega dati finanziari, relazioni societarie e interessi transnazionali.

Evasione, elusione e flussi opachi

Il bando richiama anche la capacità di leggere forme complesse di evasione ed elusione fiscale . Qui l'OSINT si intreccia con l'analisi finanziaria. Banche dati pubbliche, visure, registri internazionali, leak strutturati: tutto può diventare materia prima per ricostruire reti economiche.

Profili per diplomati: cyber e analisi operativa

Non solo laureati. Una parte della selezione è aperta a diplomati con competenze cyber e capacità di analisi di fonti aperte.

Il messaggio è chiaro: la pipeline formativa conta, ma conta anche la competenza reale.

Chi ha esperienza in:

• raccolta strutturata di dati online
• monitoraggio del deep web
• analisi di segnali digitali

può trovare uno spazio, se dimostra metodo e rigore. Il contesto europeo parla di carenza di competenze digitali avanzate. Il report ENISA evidenzia una domanda crescente nel settore cybersecurity e un gap ancora significativo tra offerta e fabbisogno.

In Italia, l'Osservatorio sulle Competenze Digitali 2025 segnala centinaia di migliaia di profili ICT mancanti.

La competizione non è solo tra Stati. È tra settore pubblico e grandi multinazionali tech. L'intelligence, per attrarre talenti, deve competere su motivazione, missione e prospettiva strategica.

Come candidarsi: passaggi operativi

1. Accesso al portale

Le candidature si presentano online nella sezione "Lavora con noi" del portale istituzionale.

Sono richieste credenziali digitali. Senza SPID o CIE, l’invio non è completabile.

2. Scadenza

Il termine è fissato alle ore 24:00 del 20 marzo 2026. Oltre quella data, la procedura si chiude.

3. Candidatura spontanea

Il DIS ricorda che resta possibile inviare candidature spontanee anche al di fuori dell’avviso mirato.

I settori citati si estendono a tecnologie dual use, sistemi satellitari, telerilevamento, lingue rare, produzione grafica e infografica.

La sicurezza nazionale è un campo ibrido. Dal codice alla geopolitica, dalle immagini satellitari ai flussi finanziari.

Pro e contro di lavorare nell’intelligence digitale

Vantaggi

Impatto strategico reale.
Accesso a contesti ad alta complessità.
Possibilità di lavorare su minacce concrete, non su simulazioni accademiche.

Criticità

Elevato livello di responsabilità.
Riservatezza stringente.
Percorsi professionali meno visibili rispetto al settore privato.

Non è una carriera glamour.
È una carriera ad alta pressione.

OSINT e sicurezza nazionale: cosa cambia

Molti cercano online: “OSINT è legale?”
Sì, se si basa su fonti pubbliche e su metodologie corrette.

La differenza sta nel metodo.
Raccogliere dati non basta. Serve verificarli, contestualizzarli, incrociarli.

Nel 2026 l’intelligence italiana manda un messaggio chiaro:
non basta avere accesso ai dati. Bisogna saperli interpretare.

https://coondivido.it/entrare-servizi-segreti-italiani/

Un segnale al mercato del lavoro

Il **Bando DIS 2026** racconta qualcosa di più di una semplice selezione.

Racconta un Paese che riconosce la centralità di:

- cybersicurezza
- open source intelligence
- analisi economico-finanziaria
- supercalcolo e intelligenza artificiale

Chi oggi studia cybersecurity, data science o OSINT si trova davanti a una domanda concreta. Non teorica.

La domanda è: vuoi mettere le tue competenze al servizio della sicurezza nazionale?

Vuoi approfondire come funziona davvero l’OSINT e quali competenze servono per lavorare tra cyber e intelligence?
Iscriviti alla newsletter OSINT & AI per Tutti su https://coondivido.substack.com/
Unisciti anche ai nostri canali Telegram:
https://t.me/osintaipertutti
https://t.me/osintprojectgroup