Come entrare nei servizi segreti italiani. Esperti OSINT e SOCMINT

Redazione | 07/05/2025 | Risorse

□□□□ Hai talento per l’OSINT? Lo Stato ti sta cercando

Cosa s□e quando i servizi segreti italiani pubblicano un annuncio di lavoro? No, non è l’inizio di un romanzo di spionaggio, ma la realtà italiana del 2025.

Il Sistema di informazione per la sicurezza della Repubblica ha lanciato un nuovo **bando mirato** per reclutare esperti di **OSINT**, **SOCMINT**, **cybersecurity** e **terrorismo internazionale**.

Un’opportunità rara, concreta, e ben documentata: vediamo chi stanno cercando e come candidarsi.

□□ Profili richiesti: non solo informatici

Il reclutamento è aperto a **diplomati e laureati** con background specifici. Ecco i profili:

□□Esperti in OSINT e Social Media Intelligence (SOCMINT)

• Titoli di studio: comunicazione, sociologia, relazioni internazionali, informatica
• Competenze chiave: ricerca avanzata online, monitoraggio social, analisi fonti aperte
• Obiettivo: produrre report strategici sulla sicurezza nazionale

□□Professionisti in cybersicurezza

• Titoli di studio: diplomi tecnici (informatica/telecomunicazioni), lauree in ingegneria, matematica, sicurezza informatica
• Skill ricercate: Penetration testing
• Red teaming
• Malware analysis
• Digital forensics
• Cyber threat intelligence

□□Tecnici delle telecomunicazioni

• Requisiti: esperienze su IP, reti RF, trasmissioni satellitari, FPGA
• Focus: progettazione e gestione di infrastrutture complesse

□□Analisti di terrorismo

• Background: lauree in discipline umanistiche o relazioni internazionali
• Competenze: conoscenza di jihadismo, radicalismi religiosi, traffico di esseri umani

© 2026 Coondivido — Tutti i diritti sono riservati

□□ Scadenze, requisiti e percorso di selezione

□□**Candidature aperte fino alle 24:00 del 10 giugno 2025**
□□ Accesso tramite SPID o CIE sul portale ufficiale:
□□sicurezzanazionale.gov.it

□□**Soft skill richieste**:

• Affidabilità e riservatezza
• Senso di responsabilità verso lo Stato
• Doti analitiche e autocontrollo

□□**Step della selezione**:

1. Screening del curriculum
2. Test psicofisici e attitudinali
3. Verifica del nulla osta di sicurezza

□□□□ Perché è un'opportunità unica (anche se non sei “007”)

La sicurezza nazionale nel 2025 non passa più solo da microspie e intercettazioni: oggi **il primo campo di battaglia è il web**.

Gli 007 italiani sanno bene che **le minacce si nascondono nei tweet, nei post criptati su Telegram, nei forum del Dark Web**. Per questo oggi cercano figure ibride, capaci di coniugare pensiero critico, tecnologia e analisi culturale.

Chi sa leggere tra le righe di un meme o analizzare una rete di contatti online può fare la differenza. Anche **senza pistola, ma con un laptop**.

□□ OSINT e SOCMINT: le competenze chiave richieste

Ecco le abilità tecniche più apprezzate nel bando:

Area	Competenze
OSINT	Google Dorks, Wayback Machine, WHOIS, Shodan, metadati
SOCMINT	Analisi reti sociali, monitoraggio hashtag, geolocalizzazione da immagini
Cybersecurity	Reverse engineering, threat intelligence, honeypot
Terrorismo e geopolitica	Analisi fonti estere, monitoraggio deep e dark web, conoscenza delle dinamiche jihadiste

□□ Chi può candidarsi davvero?

Non servono 10 anni di esperienza né carriere militari. Il bando **valorizza anche giovani professionisti**, purché dimostrino:

• Preparazione tecnica
• Etica e discrezione
• Voglia di servire lo Stato con competenze digitali

Non sei un hacker solitario. Sei un cittadino che **protegge l’Italia con il cervello, non con le armi**.

© 2026 Coondivido — Tutti i diritti sono riservati

□□ Non un lavoro qualsiasi: è una scelta

Diventare parte del comparto intelligence significa **entrare in un mondo dove ogni informazione può salvare vite**.

La selezione non è semplice. Ma è un'occasione rara, soprattutto per chi ha sempre voluto fare la differenza usando ciò che sa — e non ciò che appare.

□□ Vuoi candidarti? Fallo ora

□□ Il tempo stringe: le domande vanno inviate**entro il 10 giugno 2025**.
□□ Segui le istruzioni ufficiali su:
□□www.sicurezzanazionale.gov.it/lavora-con-noi

□□□□ Hai talento per l'OSINT? Lo Stato ti sta cercando

Cosa s□e quando i servizi segreti italiani pubblicano un annuncio di lavoro? No, non è l'inizio di un romanzo di spionaggio, ma la realtà italiana del 2025.

Il Sistema di informazione per la sicurezza della Repubblica ha lanciato un nuovo **bando mirato** per reclutare esperti di **OSINT**, **SOCMINT**, **cybersecurity** e **terrorismo internazionale**.

Un'opportunità rara, concreta, e ben documentata: vediamo chi stanno cercando e come candidarsi.

□□ Profili richiesti: non solo informatici

Il reclutamento è aperto a **diplomati e laureati** con background specifici. Ecco i profili:

□□Esperti in OSINT e Social Media Intelligence (SOCMINT)

• Titoli di studio: comunicazione, sociologia, relazioni internazionali, informatica
• Competenze chiave: ricerca avanzata online, monitoraggio social, analisi fonti aperte
• Obiettivo: produrre report strategici sulla sicurezza nazionale

□□Professionisti in cybersicurezza

• Titoli di studio: diplomi tecnici (informatica/telecomunicazioni), lauree in ingegneria, matematica, sicurezza informatica
• Skill ricercate: Penetration testing
• Red teaming
• Malware analysis
• Digital forensics
• Cyber threat intelligence

□□Tecnici delle telecomunicazioni

• Requisiti: esperienze su IP, reti RF, trasmissioni satellitari, FPGA
• Focus: progettazione e gestione di infrastrutture complesse

□□Analisti di terrorismo

• Background: lauree in discipline umanistiche o relazioni internazionali
• Competenze: conoscenza di jihadismo, radicalismi religiosi, traffico di esseri umani

□□ Scadenze, requisiti e percorso di selezione

© 2026 Coondivido — Tutti i diritti sono riservati

Candidature aperte fino alle 24:00 del 10 giugno 2025
Accesso tramite SPID o CIE sul portale ufficiale:
sicurezzanazionale.gov.it

Soft skill richieste:

• Affidabilità e riservatezza
• Senso di responsabilità verso lo Stato
• Doti analitiche e autocontrollo

Step della selezione:

1. Screening del curriculum
2. Test psicofisici e attitudinali
3. Verifica del nulla osta di sicurezza

Perché è un'opportunità unica (anche se non sei “007”)

La sicurezza nazionale nel 2025 non passa più solo da microspie e intercettazioni: oggi **il primo campo di battaglia è il web**.

Gli 007 italiani sanno bene che **le minacce si nascondono nei tweet, nei post criptati su Telegram, nei forum del Dark Web**. Per questo oggi cercano figure ibride, capaci di coniugare pensiero critico, tecnologia e analisi culturale.

Chi sa leggere tra le righe di un meme o analizzare una rete di contatti online può fare la differenza. Anche **senza pistola, ma con un laptop**.

OSINT e SOCMINT: le competenze chiave richieste

Ecco le abilità tecniche più apprezzate nel bando:

Area	Competenze
OSINT	Google Dorks, Wayback Machine, WHOIS, Shodan, metadati
SOCMINT	Analisi reti sociali, monitoraggio hashtag, geolocalizzazione da immagini
Cybersecurity	Reverse engineering, threat intelligence, honeypot
Terrorismo e geopolitica	Analisi fonti estere, monitoraggio deep e dark web, conoscenza delle dinamiche jihadiste

Chi può candidarsi davvero?

Non servono 10 anni di esperienza né carriere militari. Il bando **valorizza anche giovani professionisti**, purché dimostrino:

• Preparazione tecnica
• Etica e discrezione
• Voglia di servire lo Stato con competenze digitali

Non sei un hacker solitario. Sei un cittadino che **protegge l’Italia con il cervello, non con le armi**.

Non un lavoro qualsiasi: è una scelta

© 2026 Coondivido — Tutti i diritti sono riservati

Diventare parte del comparto intelligence significa **entrare in un mondo dove ogni informazione può salvare vite**.

La selezione non è semplice. Ma è un’occasione rara, soprattutto per chi ha sempre voluto fare la differenza usando ciò che sa — e non ciò che appare.

□□ Vuoi candidarti? Fallo ora

□□ Il tempo stringe: le domande vanno inviate **entro il 10 giugno 2025**.
□□ Segui le istruzioni ufficiali su:
□□ www.sicurezzanazionale.gov.it/lavora-con-noi

© 2026 Coondivido — Tutti i diritti sono riservati