ISACA Rome Chapter

# Newsletter

ANNO 2023 | N. 7 | LUGLIO-AGOSTO

## ISACA (Information Systems Audit and Control Association)

L'*ISACA*, (Information Systems Audit and Control Association), ha 158.998 associati in oltre 188 nazioni (dato aggiornato al 30 giugno 2023) ed è organizzazione leader nella IT Governance, Security, Controllo ed Assurance. Fondata nel 1969, ISACA promuove conferenze internazionali, pubblica riviste di aggiornamento, sviluppa standard di Audit & Controllo e amministra le certificazioni professionali *CISA* (Certified Information Systems Auditor), *CISM* (Certified Information Security Manager), *CGEIT* (Certified in the Governance of Enterprise IT), *CRISC* (Certified in Risk and Information Systems Control) e CDPSE (Certified Data Protection Solutions Engineer) . I professionisti certificati CISA (dal 1978) sono più di 99500, mentre i CISM (dal 2002) risultano a quota 21000. Le certificazioni CGEIT (introdotta nel 2007) e CRISC (introdotta nel 2010) sono rispettivamente a quota 5400 e 16000.

## EDITORIALE

# COGNITIVE WARFARE
# MIND CONTROL E NEUROWEAPONS

Parlare di Guerra Cognitiva (Cognitive warfare) e di armi neurali potrebbe sembrare fantascientifico. Purtroppo, non siamo in uno dei libri di Phil K. Dick e la questione è reale. La NATO stessa si occupa, da diversi anni, di guerra cognitiva tanto che, sul sito NATO, si trovano *articoli specifici* al riguardo: *"la guerra cognitiva incarna l'idea di combattere senza combattere. La padronanza del dominio cognitivo costituisce una nuova importante posta in gioco indispensabile per la generazione del potere del combattimento. Il Dominio Cognitivo è un nuovo spazio di competizione, oltre i domini terrestri, marittimi, aerei, cibernetici e spaziali. La guerra nel dominio cognitivo mobilita una gamma diversa e ampia di strategie, strumenti e tecniche. La sua vera essenza è prendere il controllo di luoghi, gruppi, unità, organizzazioni e nazioni, prendendo di mira e colpendo i cervelli del loro personale, civile e militare"*. Il concetto stesso di "neuro-arma" è stato *ampiamente descritta da James Giordano* e consiste quel tipo di informazione che riesce ad "accedere" al cervello e "compete" con le altre informazioni solitamente gestite dalla mente di ciascuno. D'altra parte, la neurotecnologia dual-use per la difesa è ormai da anni oggetto di numerosi programmi di ricerca DARPA e IARPA (Fonte: *the strategist*)

Vi potreste domandare cosa c'entra la guerra cognitiva e le neuro armi con le tecnologie digitali.… ebbene le tecnologie digitali hanno cambiato radicalmente la dimensione e gli ambiti della conflittualità, perché la loro pervasività ha permesso il coinvolgimento della società intera in una interconnettività globale. Notizie manipolate e diffuse digitalmente hanno modo di essere distribuite ad ampie fasce di popolazione per spostare correnti di pensiero e per influenzare e orientare giudizi. Quindi teoricamente un sempre maggior numero di persone hanno accesso alle informazioni, ma al tempo stesso, potrebbero non essere in grado di distinguere tra informazioni legittime e quelle manipolate. La guerra cognitiva si basa proprio sulla propaganda e le fake news diffuse a mezzo digitale nel web e sui social e infatti richiede l'integrazione di capacità di ingegneria informatica, informativa, psicologica sociale, condotte in sincronia con altri strumenti di potere, per influenzare atteggiamenti e comportamenti interrompendo la cognizione individuale e di gruppo per ottenere un vantaggio su un avversario. Queste attività variano notevolmente e possono comprendere componenti culturali o personalizzate: la sociologia, la teoria dei giochi e l'etica sono tutti fattori che contribuiscono ad influenzare il pensiero. La guerra cognitiva mira a colpire l'elaborazione mentale e cognitiva delle informazioni. Si estende quindi



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

oltre le conseguenze umane della guerra informatica che coinvolge ingegneria informatica, robotica e programmi; questo significa che l'hacking non è limitato ai programmi per computer, ma l'obiettivo è il cervello umano. La guerra cognitiva è quindi una forma non convenzionale di guerra che utilizza strumenti informatici per alterare i processi cognitivi nemici, sfruttare i pregiudizi mentali o il pensiero riflessivo per provocare distorsioni del pensiero, influenzare il processo decisionale e ostacolare le azioni, con effetti negativi, sia a livello individuale e collettivo.

L'aggressività cognitiva è illimitata. Può avere una varietà di obiettivi: dalla conquista territoriale (una regione confinante, una penisola o un gruppo di isole, ad esempio), all'influenza decisionale (ad esempio per orientare le elezioni o fomentare disordini popolari).(Fonte: *Dianne Marshall*) Solitamente gli avversari conducono la guerra cognitiva lungo tutto il continuum del conflitto geopolitico e mirano a rimanere in quella zona grigia, appena al di sotto del livello di un conflitto armato, o almeno quasi sempre. Purtroppo, il conflitto russo /ucraino è un esempio chiaro di questa dinamica: la Russia ha lanciato un'invasione cinetica e militare dell'Ucraina, rafforzata con attività non cinetiche, come la propaganda mirata e campagne di disinformazione e sostegno dei suoi partner. Anche la Cina usa la guerra cognitiva con una strutturale manipolazione delle informazioni concorrendo allo sviluppo di pregiudizi cognitivi interni verso il resto del mondo (disconnessione collettiva alle informazioni esterne) e di fatto, causa anche il viceversa come effetto secondario, tanto da creare progressivo effetto "noi contro di loro" e una conseguente emarginazione del popolo cinese da parte del resto del mondo, che è esattamente l'altro effetto voluto dal governo cinese per il suo popolo.

Elementi concatenati alla disinformazione cronica mirata, apportano inoltre un progressivo deterioramento della capacità di identificare i fatti dalla finzione e un conseguente decadimento della resilienza mentale, tanto che a lungo termine i destinatari tendono alla perdita di fiducia nei media.

Un ulteriore evoluzione potrebbe verificarsi con le cosiddette BCI (brain-computer-interface), mirate ad agire direttamente nella fisiologia cerebrale, secondo il criterio per cui se i pensieri sono reazioni chimiche delle cellule nervose nel cervello di una persona e seguono schemi che possono essere descritti matematicamente e se questo codice può essere letto, allora può essere hackerato, con la conseguenza che i pensieri potrebbero in linea di principio essere resi leggibili, prevedibili e quindi controllabili da un computer (Fonte: *RHC*).

Una adeguata conoscenza delle campagne di disinformazione e manipolazione potrebbe forse aiutare maggiormente, ma questo richiederebbe una sistema di monitoraggio e allerta della guerra cognitiva che necessariamente dovrebbe consentire l'identificazione di campagne di questo tipo quando si presentano e seguirle nella loro progressione, mediante una o più dashboard capaci di integrare i dati provenienti da un'ampia gamma di social media, media broadcast, social messaging e siti di social network. Ciò mostrerebbe mappe geografiche e di social network sullo sviluppo di campagne sospette nel corso del tempo. Come è facilmente comprensibile, questo tipo di monitoraggio non sarebbe troppo diverso dal sistema NSA di controllo globale, che qualche anno fa scatenò una tempesta di malcontento, per gli ovvi eccessi di sorveglianza globale che facilmente a sua volta, può essere foriera di un controllo inverso sulla popolazione mondiale. Quindi l'unica strada veramente efficace è quella di rendere i singoli più consci, più "acculturati" su queste dinamiche, più consapevoli e capaci di reagire singolarmente. Elementi di *contrasto significativo noti fin dal 2021 riguardano la diffusione della consapevolezza su queste dinamiche*, per informare e far capire come tali campagne di disinformazione possano agire. La comprensione scatena l'effetto di resilienza grazie alla capacità di distinguere fra informazioni realistiche e quelle manipolate generando una immediata o ragionata diffidenza e scetticismo o sospetto per quel genere di notizia. Di nuovo la soluzione risiede nella persona e nella sua capacità di usare l'intelletto per capire, distinguere, scegliere, perché nessuno deve abusare del singolo né per scopi malevoli, ma nemmeno per eccesso di difesa che diventa poco distinguibile dal controllo coatto. Vale sempre e oggi più che mai, la frase di Benjamin Franklin: "Chi rinuncia alla libertà per raggiungere la sicurezza, non merita né la libertà né la sicurezza". Vi esorto a ragionarci su! Se non altro è un valido esercizio per cominciare a reagire….

Alessia Valentini
Cyber security consultant, CISA



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

ISACA Rome Chapter

# Newsletter

## NOVITA' DAL CAPITOLO

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

ACCORDO

Istituto Italiano di Project Management

È stato sottoscritto un accordo tra **ISACA Roma** e l'**Istituto Italiano di Project Management® (ISIPM)**, con il quale le due associazioni intendono promuovere e sviluppare un processo di collaborazione, nelle aree culturali di comune interesse di "Project Management" e ICT Security Management, attraverso l'organizzazione e la realizzazione di attività congiunte, al fine di promuovere i principi e le tecniche professionali.

**Informiamo i Soci e i followers di ISACAROMA che stiamo proseguendo con lo svolgimento di eventi on-line. Le modalità di informazione sono le consuete mail di annuncio/invito spedite ai contatti della nostra mailing-list che coincide con la diffusione della Newsletter. Per iscriversi alla mailing list è sufficiente inviare una mail con oggetto SUBSCRIBE a *eventi@isacaroma.it*.**
**Vi terremo informati su eventuali eventi in presenza, per il momento vi auguriamo buona lettura!**

## EVENTI PASSATI

***VENERDÌ 16 GIUGNO 2023***
***15:00-17:00 (2 CPE)***

### *"LA RESILIENZA OPERATIVA DIGITALE: IL REGOLAMENTO DORA"*

*Relatore:* ***Giancarlo Butti***
*(LA BS 7799), (LA ISO IEC 27001), CRISC, CDPSE, ISM, DPO, DPO, CBCI, AMBCI.*

Con la diffusione della digitalizzazione e dei servizi ad essa collegati i settori finanziario e fintech devono attrezzarsi e imparare a reagire tempestivamente alle minacce in continuo aumento di attacchi informatici.
Nel mese di dicembre scorso sono state pubblicate nella Gazzetta Ufficiale della UE:

- il Regolamento **DORA** (Digital Operational Resilience Act) per la difesa unica europea che ha l'obiettivo di disciplinare in maniera uniforme la "resilienza operativa" nel settore finanziario in tutta l'Europa;
- la Direttiva DORA;
- ed anche la NIS2.

La documentazione degli eventi passati è disponibile sul sito *www.isacaroma.it*

## PROSSIMI EVENTI

*Con i consueti canali (mail, sito, numeri della Newsletter) vi informeremo delle prossime giornate di studio e dei seminari del nostro capitolo.*

*Gli annunci e gli inviti saranno spediti con le consuete modalità agli iscritti alla nostra mailing list.*

*I non iscritti possono ricevere tali comunicazioni inviando una mail con oggetto "subscribe" contenente solo nome e cognome a eventi<at>isacaroma.it*

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

Rome - Italy ■ 5/7 October 2023

# AEIT 2023 International Annual Conference

115th edition

## CALL FOR PAPER

Clean Electrification and Digitalization are driving forces which will shape the world. New technologies and knowledge are needed to make the world more livable and safe.

AEIT2023 International Annual Conference aims to address the main scientific and technological challenges needed today both to decarbonize the environment and to guarantee the security of energy supplies for our communities. These themes will in fact be the main themes of the conference.

AEIT2023 is an international forum dedicated to the dissemination of new ideas, research and work in progress in the sectors of integration of renewable energy, generation, transmission and distribution of energy, power systems, power electronics, automation and ICT applications. The objectives of the conference are high quality research and professional involvement between industry and academia for the advancement of science, technology and education.

The event can also be an occasion for fruitful discussions on energy plans to be developed in conditions of uncertainty in a complex world.

AEIT2023 is in its 115th edition: speakers and participants will be connected all over the world. The main features of the conference include Invited Talks, Regular Sessions, Special Sessions.

The conference will be held in presence (depending on the pandemic situation) and will also be virtual.

Organised by

AEIT 1897 — AEIT 1897 Sezione ROMA

**Tutti i dettagli li trovate qui: *https://convegni.aeit.it/AEIT2023***



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

## LE PRINCIPALI NOTIZIE

### EXPRIVIA FA IL PIEDINO AL GOVERNO SULLA CYBERSECURITY?

26 luglio – Record assoluto di attacchi cibernetici tra aprile e giugno nel nostro paese, ma la Pa migliora in sicurezza informatica. Parola di Exprivia.

È quanto sottolinea la nota del *gruppo* ICT pugliese in merito alle evidenze del nuovo 'Threat Intelligence Report' elaborato dal suo Osservatorio Cybersecurity, che prende in considerazione 129 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media.

*(source: https://www.startmag.it/cybersecurity/exprivia-fa-il-piedino-al-governo-sulla-cybersecurity/ )*

### CYBERSECURITY: CI VOGLIONO 126 GIORNI PER SANARE UNA VULNERABILITÀ CON CRITICITÀ ALTA

26 luglio – Attacchi informatici sempre più frequenti per le piccole e medie imprese italiane. Sono, infatti, aumentate del 29 per cento le attività malevole verso le pmi nel primo semestre del 2023, rispetto allo stesso periodo dell'anno precedente.

Cybergon, la business unit di Elmec Informatica dedicata alla cybersecurity, ha presentato la seconda edizione di Data Gathering, un'attività di analisi e di raccolta dati effettuata su un campione di 91 aziende capogruppo, per fornire una panoramica attuale della cybersecurity in Italia nel primo semestre dell'anno e promuovere una maggiore consapevolezza tra le diverse realtà aziendali.

*(source: https://fashionunited.it/news/moda/cybersecurity-ci-vogliono-126-giorni-per-sanare-una-vulnerabilita-con-criticita-alta/2023072624520 )*

### LA RIVOLUZIONE DELL'INTELLIGENZA ARTIFICIALE PASSA DALLA FORMAZIONE

24 luglio – È facile chiedere a ChatGPT una poesia in endecasillabi per il proprio partner, ma come la mettiamo quando si tratta di integrare i sistemi di intelligenza artificiale nei nostri strumenti di lavoro? L'AI è destinata a cambiare radicalmente il modo in cui lavoriamo e dobbiamo essere pronti a usarla nella maniera più performante possibile, sfruttando appieno tutte le sue potenzialità. È necessaria un'attività di formazione da parte delle aziende che la sviluppano. "Ogni volta che nascono nuove tecnologie le imprese si trasformano e non è mai facile", spiega Lenny Vercruysse, ceo e fondatore di Be-Cloud.

*(source: https://www.repubblica.it/tecnologia/dossier/ambizione-digitale/2023/07/24/news/la_rivoluzione_dellintelligenza_artificiale_passa_dalla_formazione-408835097/ )*

### CYBERATTACCHI, LE AZIENDE AFFINANO LE CONTROMISURE

24 luglio – Subire un attacco informatico è un rischio sempre più concreto per qualunque azienda che usi strumenti digitali. Le minacce non sono dirette solo alle large corporate, ma anche alle Pmi. Lo dimostrano i dati contenuti nel Rapporto Cyber Index Pmi realizzato da Confindustria e Generali, con il supporto scientifico dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano e la partecipazione dell'Agenzia per la Cybersicurezza Nazionale.

L'86% delle 158 Pmi con sede in Veneto che hanno partecipato al sondaggio utilizza strumenti digitali per supportare la propria attività produttiva: di queste, il 14% ha subito violazioni (ossia attacchi informatici andati a segno) negli ultimi 4 anni.

*(source: https://www.ilsole24ore.com/art/cyberattacchi-aziende-affinano-contromisure-AE2VjGxD )*

### PERCHÉ SETTE BIG TECH HANNO MESSO UN FRENO ALL'INTELLIGENZA ARTIFICIALE: COSA STA SUCCEDENDO

22 luglio – Sette aziende leader dell'intelligenza artificiale hanno deciso di salvaguardare volontariamente lo sviluppo della tecnologia. L'annuncio arriva proprio nel bel mezzo della gara. Mentre le aziende gareggiano con le nuove macchine in grado di generare mondi a partire da una stringa di testo, arriva una prima battuta d'arresto. Perché l'intelligenza artificiale non è solo questo. Dietro i chatbot geniali c'è anche disinformazione preventiva, privacy violata, lavori automatizzati, e deepfake.

Per questo **Amazon, Anthropic, Google, Inflection, Meta, Microsoft e OpenAI**, hanno deciso di aderire ai nuovi standard di sicurezza durante un incontro, venerdì 21 luglio, con Joe Biden alla Casa Bianca.

*(source: https://www.fanpage.it/innovazione/tecnologia/perche-sette-big-tech-hanno-messo-un-freno-allintelligenza-artificiale-cosa-sta-succedendo/ )*

### UN ATTACCO HACKER (TIPOLOGIA DDOS) ALLA RETE DI PUNTOZERO

22 luglio – Da venerdì 21 luglio alle ore 8:00 i nostri tecnici, con l'ausilio degli specialisti dei fornitori, sono al lavoro per mitigare un attacco hacker (tipologia DDoS) alla rete di PuntoZero che ha generato un malfunzionamento durato circa due ore, protrattosi nelle successive giornate.

**Gli apparati di sicurezza sono** riusciti **a bloccare l'ingresso ai sistemi garantendo la sicurezza dei dati** ma l'attacco ha procurato rallentamenti alla rete causando problemi di accesso ai vari servizi, tra i quali il CUP.

*(source: https://www.ospedale.perugia.it/notizie/un-attacco-hacker-tipologia-ddos-alla-rete-di-puntozero )*



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

## OTTO ITALIANI SU 10 SI SONO IMBATTUTI IN UNA MINACCIA CYBER

22 luglio – Crescono gli attacchi informatici ed il 60% degli italiani è preoccupato per la sicurezza dei propri dispositivi e prende precauzioni.

Quasi 8 su dieci si sono imbattuti in una minaccia sul web. La strada è però ancora lunga per arrivare ad una piena consapevolezza dei rischi, se si pensa che nell'ultimo anno è calata dal 58% al 50% la quota di chi afferma di avere una conoscenza a grandi linee della cybersecurity. Mentre nel 2022 il rapporto tra spesa in cybersecurity e Pil, seppure in crescita, si è attestato allo 0,1%, ponendo l'Italia come fanalino di coda tra i Paesi del G7. Ed il 52% delle imprese ha difficoltà a trovare esperti nel campo cyber.

*(source: https://www.ansa.it/canale_tecnologia/notizie/tecnologia/2023/07/22/otto-italiani-su-10-si-sono-imbattuti-nella-minaccia-cyber_04ed254b-a238-4578-b07c-51197ddb244d.html )*

## CYBER SICUREZZA: FONTI, PAPER E STUDI DI SETTORE PER RESTARE AGGIORNATI

21 luglio – Restare aggiornati, nel settore della cyber security, è fondamentale per riuscire a gestire uno scenario delle cyber minacce sempre più sofisticato e complesso.

Difatti, nell'attuale era digitale caratterizzata da una forza lavoro sempre più distribuita, da nuove modalità di interazione con i clienti e da un profondo ripensamento della supply chain, le organizzazioni si trovano a dover gestire un'importante espansione del proprio perimetro e, di conseguenza, un'esposizione maggiore ad attacchi malevoli contro il proprio patrimonio informativo.

Patrimonio informativo composto da una mole di dati in continua crescita generati sempre di più da nuove tecnologie come l'IoT (Internet of Things) che, di conseguenza, richiedono un approccio alla cyber security più evoluto rispetto al recente passato in cui lo scenario generale era decisamente meno complesso.

*(source: https://www.cybersecurity360.it/cultura-cyber/cyber-sicurezza-fonti-paper-e-studi-di-settore-per-restare-aggiornati/ )*

## INFORMARSI CON L'INTELLIGENZA ARTIFICIALE

26 luglio – Il fondatore di Notizie.it crede che si possa creare una formula per cui l'IA fa i lavori ripetitivi e i talentuosi possono fare più giornalismo di qualità. Una via stretta e un caso americano

Massimiliano Squillace ha fondato Contents.com nel marzo del 2021. All'epoca, erano in pochi a parlare di *intelligenze artificiali* generative e "*ChatGPT*" non era che un accrocco di lettere senza significato. Nel giro di circa due anni la società è diventata leader nel mercato della generazione di testi sia in Italia sia in Europa, grazie a una serie di acquisizioni, come quella della francese Scribeur o del servizio di produzione di contenuti Scribox.

*(source: https://www.ilfoglio.it/tecnologia/2023/07/26/news/informarsi-con-l-intelligenza-artificiale-5534858/ )*

## PSICOLOGIA E INTELLIGENZA ARTIFICIALE: UN'AFFASCINANTE INTERAZIONE TRA MENTE E MACCHINA

26 luglio – **L'Intelligenza Artificiale (IA)** ha fatto passi da gigante negli ultimi anni, rivoluzionando diverse aree della nostra vita, dalla ricerca scientifica all'industria, dallo sviluppo di nuove tecnologie all'*assistenza sanitaria*. Tuttavia, a misura che l'IA diventa sempre più parte integrante della nostra società, emerge la necessità di comprendere il suo impatto sulla psicologia umana e come la nostra mente interagisce con queste macchine intelligenti.

*(source: https://www.paginemediche.it/salute-digitale/psicologia-e-intelligenza-artificiale-un-affascinante-interazione-tra-mente-e-macchina )*

## DALLA STRATEGIA ALLA CERTIFICAZIONE: IL PERCORSO DI AGID PER LA PARITÀ DI GENERE

26 luglio – Parità di genere e inclusione sono temi strategici che non possono restare sulla carta ma devono tradursi in azioni concrete e misurabili. Fissare obiettivi, analizzare a che punto si è in questo percorso, intervenire sui punti deboli e continuare a lavorare per mantenere nel tempo i risultati raggiunti. È quanto sta facendo AgID, l'Agenzia per l'Italia Digitale, che lo scorso gennaio è stata tra le prime pubbliche amministrazioni centrali ad adottare il ***Piano per la parità di genere*** e ora è la prima PA ad aver ottenuto la certificazione in materia.

Ci sono numeri importanti alla base di questo primato: è donna il 42% del personale di AgID e, in particolare, è donna il 50% del personale dirigente.

*(source: https://www.forumpa.it/riforma-pa/dalla-strategia-alla-certificazione-il-percorso-di-agid-per-la-parita-di-genere/)*

## INTELLIGENZA ARTIFICIALE: GLI STEP PER UN CORRETTO TRATTAMENTO DATI

28 luglio – Sebbene la normativa sulla protezione dei dati personali europea si ispiri al principio di neutralità tecnologica, per cui i principi in esso contenuti si applicano a qualsiasi tecnica utilizzata, l'intelligenza artificiale pone sfide nuove per l'interprete e per le aziende e i professionisti che sempre più oggi si avvicinano a tale utile strumento nello svolgimento delle attività riguardanti i settori più disparati.

Ma quali sono i punti di maggiore criticità nell'utilizzo dell'IA? Quali i rischi per gli interessati? Esaminiamo **tutti gli step che il titolare dovrà seguire** per garantire la conformità del trattamento effettuato mediante strumenti di intelligenza artificiale alla normativa sulla data protection.

*(source: https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-e-data-protection-gli-step-da-seguire-per-un-corretto-trattamento/ )*



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

## ATTIVITÀ FORMATIVA DI ISACA

***INFORMAZIONI UTILI***

Chi ha già frequentato un corso a pagamento presso ISACA Roma ha uno sconto del 10%. Aziende, grossi enti, PAL, PAC e Difesa possono richiedere i costi a loro riservati alla casella **corsi<at>isacaroma<dot>it**
Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

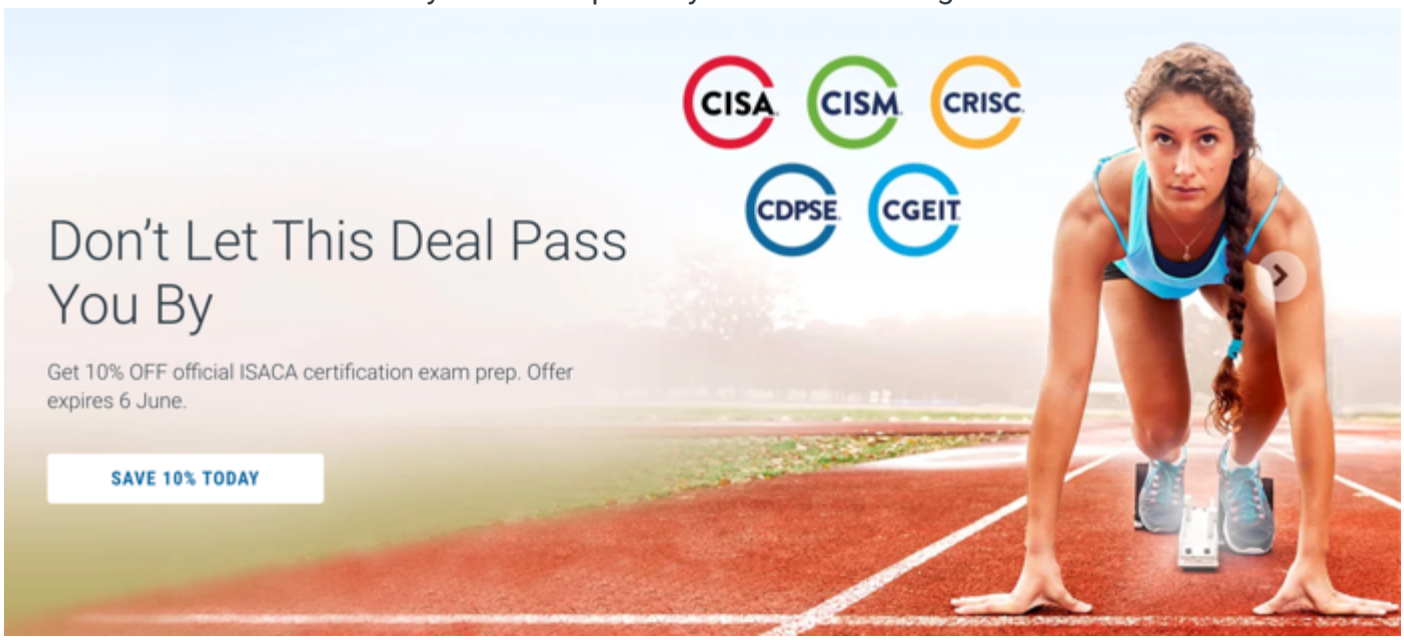
http://www.isacaroma.it/

Social Media

SAPIENZA UNIVERSITÀ DI ROMA

# WHY SHOULD I CERTIFY WITH ISACA?

Today, credentialing isn't a professional luxury—it's a career necessity. It shows you have the know-how to rise to the challenge of a modern enterprise and demonstrates your willingness to invest in yourself and commit to your industry. At ISACA, our certifications validate IT professionals like you and empower you to advance digital trust.




GET CERTIFIED



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

ISACA
Rome Chapter

# Newsletter

## ISACA CERTIFICATIONS

- CISA–Certified Information Systems Auditor
- CISM–Certified Information Security Manager
- CRISC–Certified in Risk and Information Systems Control
- CGEIT–Certified in the Governance of Enterprise IT
- CDPSE–Certified Data Privacy Solutions Engineer
- CET–Certified in Emerging Technology Certification
- ITCA–Information Technology Certified Associate
- CSX-P–CSX Cybersecurity Practitioner Certification

## ISACA CERTIFICATES

- IT Audit Fundamentals Certificate
- IT Risk Fundamentals Certificate
- Certificate of Cloud Auditing Knowledge
- Cybersecurity Audit Certificate
- Computing Fundamentals Certificate
- Networks and Infrastructure Fundamentals Certificate
- Cybersecurity Fundamentals Certificate
- Software Development Fundamentals Certificate
- Data Science Fundamentals Certificate
- Cloud Fundamentals Certificate
- Blockchain Fundamentals Certificate
- IoT Fundamentals Certificate
- Artificial Intelligence Fundamentals Certificate
- COBIT Design and Implementation
- Implementing the NIST Cybersecurity Framework Using COBIT 2019
- COBIT Foundation
- COBIT 5 Certificates

Info al sito *https://www.isaca.org/credentialing/*

ANCHE QUESTO ANNO LA NEWSLETTER DI ISACAROMA VA IN VACANZA.
CI RIVEDREMO A SETTEMBRE

Questa Newsletter è indirizzata ai soci del Capitolo di Roma di ISACA e viene anche spedita alle persone che hanno chiesto di essere inseriti nella mailing list per la comunicazione degli eventi del Capitolo.
Potete indirizzare ogni vostra richiesta (commenti, contributi, cancellazione dalla lista, ecc.) a newsletter<at>isacaroma.it.
La redazione della Newsletter è curata da Mario Taddonio (membro del CD di ISACA Roma) m.taddonio<at>isacaroma.it e da Glauco Bertocchi (VicePresidente di ISACA Roma) g.bertocchi<at>isacaroma.it
Le opinioni espresse (editoriale, ecc.) rappresentano quelle dei rispettivi autori.



ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.