ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter
Capitolo di Roma

# Newsletter

ANNO 2022 | N. 06 | GIUGNO

## ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 144.112 associati in oltre 188 nazioni (dato aggiornato a luglio 2020) ed è l'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

## LA SICUREZZA CIBERNETICA SPAZIALE

L'esplorazione è stata fondamentale per l'esperienza umana e continuerà ad ispirare molte attività umane basilari. Con questo presupposto, lo spazio assumerà sempre più importanza per la sicurezza e la prosperità globale nei decenni e nei secoli a venire.
Lo spazio è stato inestimabile per produrre ricchezza, stimolare il commercio e vincere guerre, ma un aspetto qualitativamente diverso dello spazio sta emergendo e potrebbe essere primario nel prossimo futuro. Questo nuovo paradigma per lo spazio darà priorità alla sicurezza e alle attività economiche che si verificano all'interno dello spazio stesso, non solo a quelle che si sviluppano sulla Terra.
"Lo spazio è un settore emergente di infrastrutture critiche commerciali non più dominio delle sole autorità governative nazionali" (Michael Holden – DSEI 2021). Lo spazio è un ambiente intrinsecamente rischioso in cui operare; quindi, i pericoli per la sicurezza informatica che coinvolgono lo spazio commerciale, compresi quelli che interessano i veicoli commerciali satellitari, devono essere considerati e gestiti insieme agli altri tipi di rischi per garantire operazioni sicure e di successo.
I massimi funzionari spaziali statunitensi hanno recentemente affermato che è probabile che l'invasione russa dell'Ucraina si estenderà allo spazio, prevedendo continue interferenze GPS e spoofing e sollecitando gli operatori spaziali militari e commerciali a prepararsi a possibili attacchi informatici. Il direttore del National Reconnaissance Office, Chris Scolese, ha esortato i partecipanti a una conferenza della National Security Space Association ad "assicurarsi che i vostri sistemi siano sicuri e che li stiate osservando da vicino perché sappiamo che i russi sono attori informatici efficaci".
Lo spazio è una frontiera critica della sicurezza informatica, dalla quale stiamo diventando sempre più dipendenti sia per il nostro commercio che per la sicurezza. Nella sicurezza nazionale deve essere inserita una infrastruttura critica prioritaria da proteggere.
Lo spazio sta rapidamente diventando la nuova frontiera da esplorare da parte dei governi nazionali e degli attori del settore privato. Nel processo, le diverse parti si stanno preparando per un ambiente che presenta la stessa competizione e collaborazione che sono tipiche sulla Terra e che richiederà nuovi regolamenti e norme internazionali e creerà nuove opportunità per l'industria e l'innovazione.
La nostra dipendenza dallo spazio è cresciuta esponenzialmente con la trasformazione digitale. Sfortunatamente anche i rischi, di conseguenza la necessità di dare priorità alla sicurezza informatica delle risorse spaziali è urgente. Poiché le capacità e la connettività dei dispositivi informatici sono cresciute in modo



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

esponenziale, anche le intrusioni informatiche e le minacce da malware e hacker richiedono la ristrutturazione delle priorità.
La minaccia informatica include varie imprese criminali e stati nazionali avversari. Proteggere le risorse spaziali dalle minacce informatiche è un imperativo di sicurezza nazionale. Mentre investiamo e continuiamo a costruire la spina dorsale satellitare che guiderà la nostra sicurezza e il nostro benessere economico per i prossimi decenni, la sicurezza cibernetica spaziale già in fase di progettazione non può che essere un requisito indispensabile.

**Alberto Traballesi**
In servizio presso l'Aeronautica Militare Italiana dal 1958 al 1995, ha lasciato il servizio attivo con il grado di Generale di Brigata Aerea. Sino al 2013 ha servito come esperto presso la Presidenza del Consiglio dei Ministri. Laureato in Matematica, Ingegneria elettronica e Scienze Aeronautiche. Attualmente è parte attiva in ricerche sulla protezione delle IC e sulle tematiche spaziali.
È vice-presidente AIIC.

## 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.
L'intenzione è quella di:

- avvicinare le community nazionali di **ISIPM** e **ISACA**
- ampliare le aree di interesse delle due community
- favorire lo scambio di esperienze e conoscenze
- aumentare il grado di formazione e di competenza nelle tematiche di interesse delle due organizzazioni
- organizzare congiuntamente eventi e/o webinar di "Project Management" e ICT Security Management, per sensibilizzare i propri soci sull'importanza di tali discipline e delle relative metodologie e tecniche.
- sviluppare percorsi formativi congiunti, che uniscano la formazione per le certificazioni di **ISACA (CSX® fundamentals**, **CSX-P**, **CISA®**, **CISM®**, **CGEIT®** e **CRISC®)**, a quella per la certificazione **ISIPM-Base®** e alla qualificazione **ISIPM-Av®** di **ISIPM** (1° e 2° livello di certificazione PM). L'obiettivo è fornire le competenze organizzative, tecniche, ed operative in materia di **Cyber-Security,** insieme alle conoscenze di **Project Management**, utili e necessarie per coloro che partecipano a progetti in vari ruoli o intendono qualificarsi.
- sviluppare e sostenere gruppi di lavoro congiunti, per studiare e creare nuove opportunità, che possono avvicinare sempre di più le due discipline, su obbiettivi comuni.

**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!**


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

CSX P™
Certified Cybersecurity Practitioner

ISACA Roma ha attivato il percorso, teorico e pratico con esercitazioni, per ottenere la certificazione "CSX Practitioner Certificate". Il capitolo di Roma è uno dei pochi in Europa e nel mondo ad aver completato l'iter che consente di erogare lezioni anche on-line e di fornire agli studenti la possibilità di esercitarsi con 70 laboratori virtuali.

CSX-P è stato introdotto da ISACA nel 2015 certificazione indipendente dai fornitori e basata sulle abilità a risolvere problemi, per i professionisti dell'information security e cybersecurity. CSX-P richiede ai candidati di dimostrare le proprie capacità nella cybersecurity in un ambiente dinamico e virtuale, cimentandosi su scenari attuali di cyber security, e non semplicemente superare un esame con domande a risposta multipla.

È la sola certificazione completa basata sulle performance individuali nel settore che verifica l'abilità del candidato di svolgere compiti tecnici nelle cinque funzioni di sicurezza definite dal framework NIST – identify, protect, detect, respond and recover. Ai candidati è richiesto di mettere in pratica le competenze acquisite sulla cybersecurity e dimostrare di possedere le abilità necessarie per reagire a un ambiente di minacce cyber sempre più aggressivo e vario.

CSX Practitioner Certificate consiste nel:

1. risolvere i compiti presenti in 10 laboratori virtuali

2. superare l'esame

3. dimostrare di possedere i requisiti per la certificazione (esperienza pluriennale, possesso di ulteriori certificazioni).

Sono disponibili due tipologie di laboratori virtuali:

- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori indipendenti e utilizzabili off-line.

È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi.

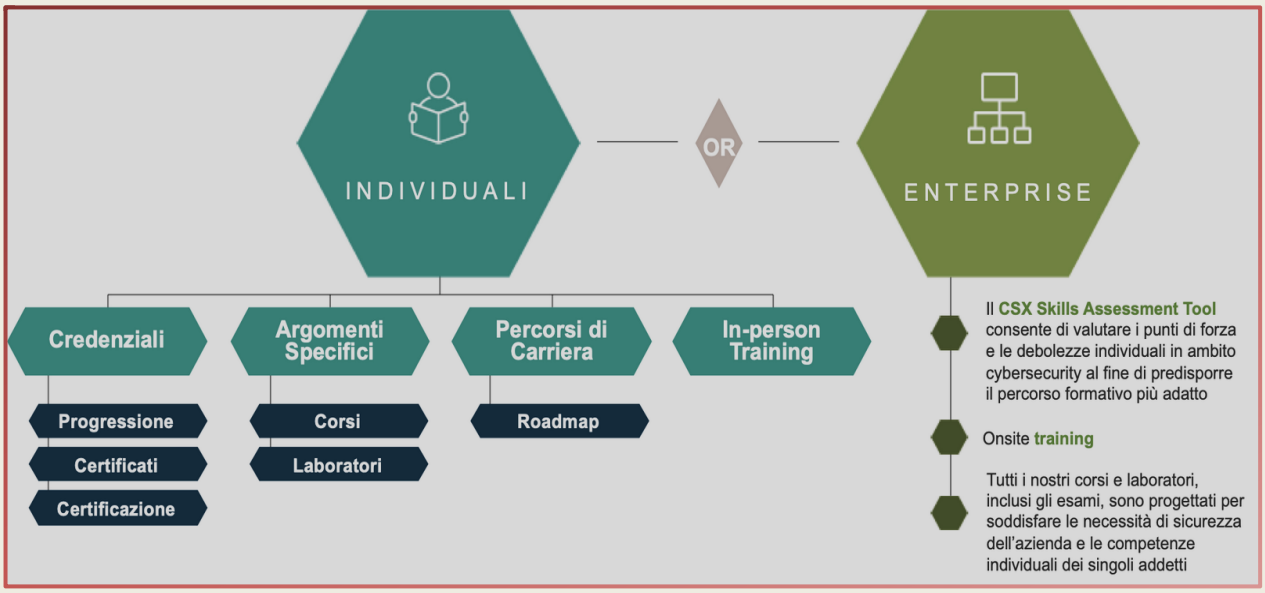
Il partecipante svilupperà competenze pratiche sulla cybersecurity oltre a una solida base teorica, il 50% di tutti i corsi comprende degli esercizi pratici di laboratorio in un **cyber ambiente virtuale**. Nello stesso tempo si approfondiranno le tecniche per rispondere agli attacchi e recuperare dati e sistemi in caso di disastro, in particolare:

- Network evaluation
- Vulnerability analysis
- Malware & incident detection
- Incidence reporting
- Safeguard implementation.

L'offerta di corsi CSX è molto varia e modulare, ciò consente anche un approccio graduale e focalizzato su specifici ambiti (penetration e vulnerability, analisys, specialist) per consentire una formazione finalizzata qualora necessaria.



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




Maggiori dettagli sono disponibili*about:blank* qui:
*http://www.isacaroma.it/wp-content/uploads/2019/11/CILLI-CSX_Training_Options_IT.pdf*
**ISACA Roma**

- **Segreteria Corsi**
- **Tel. +39 375 599 1500**
- **cybersecurity@isacaroma.it**

***www.csxp.it***

## EVENTI PASSATI

***VEN 01 LUGLIO 2022***
***ORE 15:00-17:00***

# "INSERT COIN TO CONTINUE... IL RANSOMWARE NEL GAMING"

*"Un recente ingaggio nel mondo del gaming online mi ha introdotto ad alcune pratiche proprie di questa industria che, se da un lato applica stringenti controlli applicativi, dall'altra sembra essere piuttosto rilassata nei confronti della gestione delle infrastrutture... come mi ha potuto dimostrare una famosa gang di ransomware..."*

**Il relatore:** ***Stefano Maccaglia***
***È Senior Principal Consultant nel team di Incident Response di RSA dal 2012 e ha alle spalle numerose investigazioni su incidenti di grandi dimensioni in varie parti del mondo. Hacker della prima ora, nonche' antropologo e sociologo, nel suo percorso lavorativo ha collaborato con molte realta' di primo piano del panorama ICT mondiale, da Digital a Cisco. Speaker abituale di conferenze internazionali, al di fuori del lavoro e' attivo nella produzione di contributi sulle tematiche della cybersecurity e del cyber-spionaggio.***

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

## PROSSIMI EVENTI



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

***16 Settembre 2022***
***ore 15,00-17,00***

## "LE ANALISI DEI RISCHI NEL GDPR"

*A differenza della DPIA (art. 35) che deve essere eseguita solo nei casi espressamente previsti dalla normativa o quando si è in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, le analisi dei rischi previste dagli artt. 24, 25 e 32 del GDPR sono sempre obbligatorie, per lo più disattese, e non riguardano solo aspetti di sicurezza.*

*Vi è quindi una diffusa incoerenza fra quanto richiesto dalla normativa e quando effettivamente agito. Se da un lato questo si traduce in una estesa mancanza di conformità da parte dei Titolari, dall'altro risultano carenti le adeguate misure tecniche ed organizzative poste a tutela delle persone fisiche ed il loro diritti.*

*Qual è quindi il corretto approccio a questi adempimenti e quali sono gli strumenti che il Titolare ha a disposizione?*

**Il relatore: Giancarlo Butti**

***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***

## LE PRINCIPALI NOTIZIE

### CYBER SECURITY NEL SETTORE SPAZIO: TECNICHE DI ANALISI E DIFESA

22 giugno 2022 – Il settore Spazio è ormai diventato di importanza strategica: l'incidente di sicurezza accaduto all'inizio della guerra in Ucraina proprio a un'infrastruttura satellitare ne è la dimostrazione. E la futura connettività alle reti 5G, l'ingresso di nuovi attori privati e la crescente presenza di nuovi paesi emergenti non faranno altro che aumentare la superfice di attacco. Ecco i punti su cui intervenire.

*(source: https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-nel-settore-spazio-tecniche-di-analisi-e-difesa/ )*

### CYBERSICUREZZA: IL CENTRO DI VALUTAZIONE E CERTIFICAZIONE

04 luglio 2022 – L'Agenzia Nazionale per la Cybersicurezza ha fatto sapere che è dal primo luglio 2022 operativo il **Centro di valutazione e certificazione nazionale**. Questo Centro di valutazione e certificazione (Cvcn) sarà inlcuso nel Servizio certificazione e vigilanza. Il direttore è **Andrea Billet.** Scopriamo più nel dettaglio quali sono gli ambiti di cui si occuperà il CVCN e quali sono gli obiettivi che l'Agenzia si è fissata.

*(source: https://sicurezza.net/cyber-security/cybersicurezza-operativo-centro-valutazione-certificazione/#gref )*

### STARTUP, DIGITHON: TRA CYBERSECURITY E METAVERSO PRONTI PER MARATONA DA 7 A 10 LUGLIO A BISCEGLIE

01 luglio 2022 – Tutto pronto alle Vecchie Segherie di Bisceglie per DigithON 2022, la più grande maratona digitale italiana che torna in presenza, dal 7 al 10 luglio: quattro giorni non-stop con una full immersion nel mondo del digitale, 48 ore di competition tra le 100 startup finaliste, confronto con le aziende, formazione, grandi eventi e momenti di approfondimento con nomi di primo piano delle istituzioni e delle imprese.

*(source: https://www.today.it/partner/adnkronos/economia/lavoro/startup-digithon-tra-cybersecurity-e-metaverso-*



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

*pronti-per-maratona-da-7-a-10-luglio-a-bisceglie.html )*

## OPERATIVO IL CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE (CVCN): UN TRAGUARDO PER LA CYBER NAZIONALE

06 luglio 2022 – I **l Centro di Valutazione e Certificazione Nazionale (CVCN)**, così come previsto dalla normativa in ambito Perimetro di Sicurezza Nazionale Cibernetica (PSNC) nonché dal D.L. n. 82 del 2021, è ora **operativo** e collocato all'interno del Servizio Certificazione e Vigilanza dell'Agenzia per la Cybersicurezza Nazionale (ACN). Tale passaggio si pone come un elemento imprescindibile per la piena istituzione del Perimetro di Sicurezza Nazionale Cibernetica.

*(source: https://www.cybersecurity360.it/cybersecurity-nazionale/operativo-il-centro-di-valutazione-e-certificazione-nazionale-cvcn-un-traguardo-per-la-cyber-nazionale/ )*

## DIGITAL360 SPINGE SULLA CYBERSECURITY: ACQUISIRÀ IL 75% DI CRYPTONET

30 giugno 2022 – Grazie all'acquisizione di CryptoNet si costituisce in Digital360 un polo di servizi dedicato alla cybersecurity, con un fatturato complessivo atteso nel 2022 di 5,5 milioni di euro, una crescita superiore al 25% rispetto al 2021, di cui quasi la metà ricorsivi.

*(source: https://www.techcompany360.it/fusioni-acquisizioni/digital360-spinge-sulla-cybersecurity-acquisira-il-75-di-cryptonet/)*

## CYBERSECURITY, PERCHÉ PUNTARE SU FORMAZIONE E PROMOZIONE DELLA CULTURA

30 giugno 2022 – Il Governo, di recente, ha lanciato la nostra nuova **"Strategia Nazionale di Cybersicurezza 2022-2026"**, predisposta grazie al contributo dell'**Agenzia per la Cybersicurezza Nazionale (ACN)** e al coordinamento dell'**Autorità delegata per la sicurezza della Repubblica Franco Gabrielli**, la quale prevede un vastissimo ventaglio di misure implementative (ben 82) tese ad innalzare nel corso dei prossimi anni il livello di "cyber resilienza" del nostro Paese.

*(source: https://www.econopoly.ilsole24ore.com/2022/06/30/cybersecurity-strategia-nazionale/ )*

## AUMENTANO I CRIMINI SU SOCIAL MEDIA, MA I TRUFFATI NON DENUNCIANO

01 luglio 2022 – Secondo una statistica di **SmartinsIghts** oltre la **metà della popolazione globale usa i social media (il 58,4%, pari a 4.62 miliardi di persone)**, l'utilizzo **medio giornaliero è di 2 ore e 27 minuti**.

Queste piattaforme sono però diventate sempre più **un grimaldello per i cybercriminali** per risalire alle abitudini degli utenti e alle password usate. Per questo gli esperti della società di sicurezza consigliano di **limitare la condivisione di informazioni personali**, **usare email, login e password diverse per i differenti servizi che usiamo**, costruire **password lunghe**, **robuste** e **complesse** senza riferimento a hobby, passioni e residenza.

*(source: https://www.cybersecurity360.it/nuove-minacce/furti-di-account-whatsapp-ecco-come-proteggersi-dalla-nuova-cyber-truffa/ )*

## CHE COSA SAPPIAMO SU UNO DEI FURTI DI DATI PIÙ GRANDI DELLA STORIA

06 luglio 2022 – Più di 23 terabyte di dati appartenenti **a un miliardo di cittadini cinesi** sarebbero stati sottratti da un hacker da un database della polizia di Shanghai. Se la violazione venisse confermata, sarebbe una delle più gravi della storia. Al momento non ci sono dichiarazioni ufficiali da parte delle autorità della Repubblica Popolare. Il cybercriminale si è identificato solamente come ChinaDan.

*(source: https://www.wired.it/article/chinadan-furto-di-dati-piu-grande-della-storia/ )*

## THE CASE FOR OUTCOME-BASED CYBERSECURITY: A DATA-FOCUSED SHIFT IN CYBERSECURITY MANAGEMENT

01 luglio 2022 – The challenges faced by today's cybersecurity practitioners are well documented, however, the situation may be worse than described. It is not just that cybersecurity is extremely complex, that compliance requirements and the cost of noncompliance both continually escalate, that cybersecurity threats evolve at breath-taking rates or that all of this has to be managed with increasingly limited pools of cybersecurity personnel and constrained financial resources. The frightening truth is that all of these problems are simultaneously relevant. It is a perfect storm, and there is little reason to expect it will change if the global cybersecurity community continues to embrace the status quo.

*(source: https://www.isaca.org/resources/news-and-trends/industry-news/2022/the-case-for-outcome-based-cybersecurity )*

## CYBERSECURITY E SOSTENIBILITÀ POSSONO COESISTERE? L'AGENDA 2030 DICE SÌ!

04 luglio 2022 – Sono forse due degli argomenti più discussi, cliccati, e ricercati del nuovo millennio: parliamo di cybersecurity, sicurezza cibernetica in italiano, e sostenibilità. Il primo termine è strettamente legato alla tecnologia, il secondo alla natura, ma che grazie alla tecnologia può migliorare. Possono questi due mondi in qualche modo coesistere e collaborare? E se sì, in che modo? Vediamolo insieme, grazie anche all'Agenda 2030 delle Nazioni Unite.

*(source: https://www.ecodallecitta.it/cybersecurity-e-sostenibilita-possono-coesistere-lagenda-2030-dice-si/ )*



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

## CORSI ISACA

### L'ATTIVITÀ FORMATIVA DI ISACA ROMA NON È SOSPESA!

### I CORSI SONO EROGATI IN MODALITÀ ONLINE

**LA NUOVA CERTIFICAZIONE CSX-P (CYBERSECURITY PRACTITIONER)**

*Per ulteriori informazioni visitare il sito dedicato alla certificazione CSX-P (www.csxp.it).*

***ULTERIORI INFORMAZIONI SUI CORSI NELLE SEZIONI SPECIFICHE DEL SITO WWW.ISACAROMA.IT***

**Cybersecurity Nexus (CSX)** è il programma professionale di ISACA Intl con il quale verranno sviluppate le conoscenze per una corretta gestione della sicurezza informatica. Il programma CSX è il risultato dell'esperienza ultradecennale maturata da ISACA Intl nelle attività di auditing, di gestione dei rischi, del security management e del'IT governance. CSX sta aiutando a plasmare il futuro della sicurezza informatica.

***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

Social Media

http://www.isacaroma.it/

SAPIENZA
UNIVERSITÀ DI ROMA

### CISA, CRISC, CISM, CGEIT, CSX-P O CDPSE
### DOPO IL TUO NOME DIMOSTRA CHE HAI LE COMPETENZE PER AFFRONTARE LE SFIDE DELL'AZIENDA MODERNA:

**GET CERTIFIED**



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

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

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.