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

Newsletter

ANNO 2023 **N. 1** **GENNAIO**

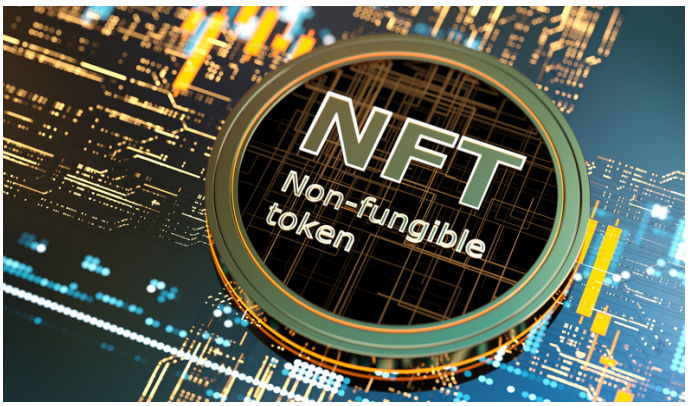
ISACA (Information Systems Audit and Control Association)

L'*ISACA*, (Information Systems Audit and Control Association), ha 160.296 associati in oltre 188 nazioni (dato aggiornato al 31 ottobre 2022) 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 DEI NON FUNGIBLE TOKENS (NFT)

La tecnologia dei Non Fungible Token (NFT, letteralmente gettone non fungibile n.d.r.) esiste dal 2012 come "invenzione del concetto teorico", ma il primo NFT Token su blockchain è stato creato nel 2014 (Fonte *Trend-online*).



L'NFT è il mezzo per rappresentare la proprietà di oggetti unici, ma in sostanza gli NFT sono risorse digitali, come foto, video, file audio o un altro formato digitale e si possono applicare a opere d'arte, fumetti, oggetti sportivi da collezione, carte collezionabili, giochi e perfino immobili. La dicitura "Non fungibile" è un termine economico che indica la caratteristica di non intercambiabilità con altri tokens (gettone n.d.r.). I token non fungibili o NTF sono risorse crittografiche che si trovano su una blockchain (un registro distribuito o se si preferisce un libro mastro pubblico distribuito che registra le transazioni a cui l'NFT è legato n.d.r.). La proprietà di un bene NFT è garantita dalla blockchain perché nessuno può modificare il registro di proprietà o copiare/incollare un nuovo NFT. Ogni NFT contiene codici identificativi univoci per poterli distinguere uno dall'altro. Questi dati facilitano il trasferimento dei token tra i proprietari e la verifica della proprietà. Per comprare e vendere NFT si usano marketplace ovvero mercati digitali che consentono lo scambio mediante l'uso di portafogli digitali (crypto wallets) per l'uso dei quali è sempre necessario avere un crypto exchange account.

Gli NFT e le criptovalute condividono alcune somiglianze ma hanno anche importanti differenze: la principale è che le criptovalute sono fungibili e gli NFT, non sono fungibili; quindi, un Bitcoin equivale a un altro Bitcoin, ma un NFT non equivale a un altro NFT. Ogni asset NFT è unico e il suo valore è determinato dalle forze di mercato (domanda/offerta n.d.r.).

Sebbene la tecnologia esista da un po' di tempo, gli NFT sono decollati nel 2020 e da allora sono diventati sempre più popolari, in particolare nel mondo dell'arte digitale. Nonostante il grande entusiasmo che li ha ammantati, sono stati oggetto di molte critiche per la loro caratteristica di essere volatili, altamente speculativi e purtroppo anche vulnerabili alle truffe.

Le truffe possono interessare ogni aspetto degli scambi, degli account utente, possono essere perpetrati verso i marketplace di scambio ma possono anche essere indirizzati sui portafogli digitali dei singoli utenti. Attualmente i marketplace più famosi sono OpenSea, NBA Top Shot, Nifty Gateway, Rarible. Proprio su OpenSea lo scorso anno, a febbraio, è avvenuto l'incidente di sicurezza più ingente di questa area tecnologica: il furto di NFT per un bottino da 1,5 milioni di euro. Secondo le prime analisi i criminali digitali avrebbero sfruttato impropriamente una caratteristica del Wyvern Protocol, (standard open-source n.d.r.) usato da molte piattaforme che hanno a che fare con la

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

blockchain Ethereum usata per la gestione dei contratti. Gli utenti sarebbero stati indotti a firmare un accordo parziale che autorizzava il trasferimento di NFT, senza il corrispettivo trasferimento di ETH (crypto moneta ethereum n.d.r.) (Fonte *HD blog*).
A parte le singole occorrenze di incidenti, le principali truffe che possono interessare l'ambito tecnologico degli NFT includono:

- Truffe di phishing: collegamenti ingannevoli e pop-up che promuovono nuovi progetti NFT per adescare utenti interessati anche via social media.
- Catfishing: falsi siti Web di mercato, falsi account di social media e imitatori di celebrità che pubblicizzano NFT per invogliare gli utenti a comprarli.
- NFT contraffatti: i criminali agiscono vendendo NFT prodotti da altri spacciandosi per i veri creatori del lavoro originale.
- Schemi pump-and-dump: i truffatori creano clamore attorno a un NFT in modo che venga venduto a un prezzo elevato, ma poi incassano rapidamente, lasciando gli investitori con risorse senza valore.
- Truffe di "conio" gratuito: i truffatori utilizzano tattiche ingannevoli, manipolatorie per fare pressione sugli investitori e spingerli a partecipare al conio di NFT originali, ma invece di ricevere il nuovo NFT, la vittima rinuncia, senza rendersene conto, al diritto di controllare il proprio portafoglio, che viene quindi svuotato dai criminali.

Le prassi di sicurezza per prevenire incidenti di sicurezza legati agli NFT (Fonti *Kaspersky*, *Imperva,* *Cloudwards*) richiedono di:

- Usare sempre password complesse e autenticazione a due fattori per gli account usati per gli acquisti di NFT
- Conservare gli acquisti in un "cold wallet", ovvero un dispositivo hardware in cui le chiavi e le risorse sono archiviate offline (per evitare esfiltrazioni di valori monetari on line), usando un wallet di scambio in cui tenere "pochi spiccioli".
- Effettuare preventivamente una transazione iniziale con una piccola somma di denaro per assicurarsi che tutto funzioni correttamente, al fine di evitare investimenti di somme significative "al buio".
- Ignorare lo spam, i messaggi diretti o strani NFT che estranei inviano al proprio portafoglio e a cui potrebbero essere allegati contratti dannosi.
- Verificare la protezione delle proprie informazioni e della criptovaluta di scambio, prima di acquistare NFT.
- Informarsi mediante guide online e recensioni per comprendere il mercato e i rischi connessi.

Per approfondimenti su NFT è possibile consultare la *Ethereum org*

Alessia Valentini
Cyber security consultant, CISA

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!

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

EVENTI PASSATI

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

PROSSIMI EVENTI

VENERDÌ 27 GENNAIO 2023 15:00-17:00 (2 CPE)

"LA CORSA VERSO NUOVI MONDI E LA CYBERSECURITY"

L'occasione di questo webinar nasce dal sempre maggior rilevo delle esplorazioni spaziali e dalle prospettive di crescita del settore a breve e a medio termine. Lo studio e l'esplorazione dei corpi celesti nel nostro sistema solare hanno condotto all'individuazione di possibili destinazioni d'interesse per le attività dell'uomo; verso le quali effettuare i primi passi al di fuori del pianeta Terra. Si tratta dell'individuazione di obiettivi, viaggi su pianeti del sistema solare, che richiedono la soluzione di problematiche molto complesse sia per raggiungerli che per abitarli per tempi più o meno lunghi. I fattori abilitanti sono rappresentati da tecnologie in grado di rispondere agli elevatissimi requisiti di affidabilità e resilienza richiesti per tali missioni spaziali. Tra queste tecnologie c'è sicuramente l'ICT nella doppia accezione di informatica e telecomunicazioni e quindi ecco entrare in campo anche le esigenze di cybersecurity, resilienza, ecc. Il webinar è l'occasione per uno sguardo panoramico su un possibile prossimo futuro in un'ottica di interdisciplinarità.

Relatori:
Gen. B.A. (c) 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 vicepresidente AIIC.
Ing. Roberto Sommma
Entrato in Selenia (oggi Thales Alenia Space) nel 1970 subito dopo la laurea in Ingegneria Elettronica, si è occupato fino al 1980 di Affidabilità dei Sistemi Spaziali. Gli è stata quindi affidata la responsabilità dello sviluppo de settore Telerilevamento, nel quale ha varato e diretto lo sviluppo dei radar spaziali. Dirigente dal 1985, nel 1991 ha avuto la direzione operativa della nuova Divisione Telerilevamento. In pensione a fine 2007, è rimasto in azienda fino al 2014 come Senior Advisor dell'Amministratore Delegato

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.

LE PRINCIPALI NOTIZIE

NON-FUNGIBLE TOKENS FOR THE MANAGEMENT OF HEALTH DATA

23 gennaio – The COVID-19 pandemic stimulated an unprecedented push for digital transformation, accelerating the adoption of digital technology in health care. There was a surge in telemedicine services, in artificial intelligence (AI) for SARS-CoV-2 detection, and in the use of AI to predict blueprints for vaccine development. With the increased digital flow of data, there is a need for privacy-preserving technologies to improve research and clinical applications within the healthcare system. Data tokenization on the blockchain provides high levels of privacy and confers the potential for personal ownership of health data, which other privacy-preserving technologies such as federated learning and generative adversarial networks do not offer (see Table *1* for a glossary of terms). The use of **non-fungible tokens (NFTs)** is a potential data-management solution for the governance of data at both personal and institutional levels.
(source: https://www.nature.com/articles/s41591-022-02125-2)

CHATGPT, ORA BASTA GIOCARE: ECCO UTILIZZI E RISCHI (SERI)

20 gennaio – **ChatGPT** è l'argomento del momento, perché sembra che l'*Intelligenza artificiale* (IA) sia salita un altro gradino della *propria scala evolutiva*.

Per capire meglio come funziona, quali potenzialità offre e quali rischi comporta, occorre osservarla da vicino nel modo più neutrale e distante possibile, lasciandosi stupire, positivamente o meno, dai risultati che restituisce. Considerando le sue doti di conversazione e il contesto, nessuno meglio di ChatGPT può spiegare cosa è davvero in grado di fare.
(source: https://www.agendadigitale.eu/mercati-digitali/chatgpt-ia-generativa-openai/)

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE

21 gennaio – Il Dipartimento dell'Istruzione di New York la mette al bando ma Microsoft la finanzia, per Bloomberg segna l'inizio di una rivoluzione nei costumi ma il New York Times la considera "un pericolo per la democrazia": il primo tema rovente del 2023 sul quale l'America si divide è ChatGPT, lo strumento digitale che consente a chiunque di ricorrere all'intelligenza artificiale per creare - con una semplice domanda - qualsiasi tipo di contenuto intellettuale, dagli articoli alle poesie, dalle formule ai quadri.
(source: https://www.repubblica.it/editoriali/2023/01/21/news/chatgpt_intelligenza_artificiale_america_molinari-384536740/)

LACRIME NEL CYBERCRIME: I RICAVI DEL RANSOMWARE CROLLANO DEL 40% NEL 2022

22 gennaio – Il 2022 è stato un anno importante nella lotta al ransomware. Secondo le *statistiche di Chainalysis*, i cyber-criminali di tutto il mondo sono riusciti a ottenere un totale di circa **457 milioni di dollari nel 2022**. Queste cifre, come da previsione nel 2020 e nel 2021 si sarebbero dovute attestare intorno agli 800 milioni di dollari. Di fatto abbiamo assistito ad un calo esponenziale, pari a quasi il 40%.
È chiaro che è impossibile registrare tutti i crimini informatici che si verificano nel mondo, ma anche secondo le informazioni di pubblico dominio, c'è una chiara tendenza: **il reddito degli hacker criminali è diminuito drasticamente nel 2022.**
(source: https://www.redhotcyber.com/post/lacrime-nel-cybercrime-i-ricavi-del-ransomware-crollano-del-40-nel-2022/)

LA RIVOLUZIONE DEL DIGITALE PUBBLICO: PARTE IN QUESTI GIORNI LA VALUTAZIONE DEL RISCHIO PER I DATI

22 gennaio – Tre profili di rischio per una protezione centralizzata della futura amministrazione pubblica digitale: inizia in questi giorni la rivoluzione digitale delle amministrazioni italiane, che si sposteranno sui server dei quattro datacenter che formano il nuovo Cloud Nazionale.
Ora, dopo l'accensione dei server avvenuta a fine dicembre, tocca all'Agenzia per la Cybersicurezza Nazionale, cui compete la strutturazione della sicurezza dei dati.
Dal 19 gennaio ha preso il via la fase forse più impegnativa, quella della catalogazione di tutti i dati in base al profilo di rischio, oltre alla validazione e alla qualificazione - da parte dell'Agenzia - dei service cloud e delle infrastrutture.
(source: https://it.euronews.com/2023/01/22/la-rivoluzione-del-digitale-pubblico-parte-in-questi-giorni-la-valutazione-del-rischio-per)

WHATSAPP SI BECCA UNA MULTA DA 5,5 MILIONI DI EURO PER VIOLAZIONI DEL GDPR

22 gennaio – Continua a piovere sul bagnato per il gruppo ***Meta***: dopo la ***sanzione di 390 milioni inflitta dall'UE*** per **violazione del GDPR** attraverso gli annunci personalizzati, la *Data Protection Commission* (DPC) irlandese ha inflitto una nuova **multa da 5,5 milioni di euro** a WhatsApp, la famosa piattaforma di messaggistica che fa capo proprio a Meta.
La sanzione è stata comminata dopo la **conclusione di un'inchiesta su WhatsApp Ireland Limited** in relazione alla fornitura del suo servizio ***WhatsApp*** con il quale avrebbe violato il **GDPR**; la commissione ha inoltre richiesto all'azienda di adeguare la piattaforma, concedendo sei mesi di tempo per rendere conformi le proprie operazioni legate al trattamento dei dati.
(source: https://www.tuttoandroid.net/news/2023/01/22/violazione-gdpr-whatsapp-multa-dpc-irlandese-978162/)

DATA MANAGEMENT, SCOPRIAMO COME CAMBIERÀ NEL 2023

20 gennaio – La sempre maggiore quantità di big data sta spingendo le aziende a investire maggiormente in strumenti e tecnologie per la loro gestione, ai fini di utilizzare tutti i dati a disposizione per migliorare le operazioni, comprendere meglio i clienti, consegnare i prodotti più velocemente e ottenere altri vantaggi aziendali attraverso le applicazioni di analisi.

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

Ovviamente, tutto ciò presuppone una gestione strutturata dei dati in conformità con le vigenti normative.
(source: https://www.cybersecurity360.it/outlook/data-management-scopriamo-come-cambiera-nel-2023/)

CYBER SECURITY 2023, PER DIFENDERSI È CRUCIALE LA GESTIONE DEGLI ASSET

13 gennaio – L'umanità ha interesse ad avere un ecosistema digitale il più salubre possibile fino a definire la sicurezza digitale un bene dal valore intrinseco. Ci aiuteranno, tra gli altri, l'Intelligenza artificiale e la nostra capacità di saper gestire il rischio nelle organizzazioni.
Il processo di trasformazione digitale ha reso l'intero sistema economico, sociale e politico fortemente dipendente in maniera irreversibile dalla interconnessione di intelligenze distribuite in ogni angolo del pianeta e dello spazio abitato e non, dal macrocosmo al microcosmo.
(source: https://www.cybersecurity360.it/outlook/cyber-security-2023-per-difendersi-e-cruciale-la-gestione-degli-asset/)

L'AGENZIA NAZIONALE PER LA CYBERSICUREZZA CERCA ACCELERATORI DI STARTUP

19 gennaio – **Al via il piano per le startup dell'Agenzia per la cybersicurezza nazionale** (ACN). L'ente preposto a stabilire regole e strategie per la cybersecurity italiana *ha pianificato di costituire una rete di collaborazioni*, il **Cyber innovation network**, **per il lancio di programmi nel settore della cybersicurezza** che hanno lo scopo di sviluppare startup impegnate a valorizzare tecnologie tra cui la **data science, la robotica, la blockchain, l'intelligenza artificiale, l'Internet of things, la computazione quantistica** e **la crittografia.**

(source: https://www.wired.it/article/startup-cybersecurity-agenzia-bando-incubatori-acceleratori/)

COME DARE LE "ISTRUZIONI GIUSTE" A CHATGPT

23 gennaio – Alzi la mano chi non ha provato almeno una volta a creare ***un testo con ChatGPT***. La soluzione di ***generative Ai*** messa a disposizione da ***OpenAi*** ha avuto il merito di rendere l'***intelligenza artificiale*** più familiare ai non addetti ai lavori. Anche chi non ha competenze di programmazione può oggi fare scrivere al computer una email, una brochure commerciale, un testo per il proprio blog: basta **dare le istruzioni giuste** e scegliere fra i diversi testi che la macchina restituisce. Tutto questo si applica anche alle **immagini**, alla **musica**, ai **video** e ai **codici di programmazione**.
(source: https://www.wired.it/article/chatgpt-istruzioni-giuste-come-dare/)

PROTOCOLLO DI INTESA TRA CISCO E L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

23 gennaio – Solo qualche settimana fa avevamo dato notizia dell'alleanza tra l'Agenzia per la ***Cybersicurezza*** Nazionale (ACN) e Microsoft con l'obiettivo di agire in maniera preventiva e mitigare i rischi legati all'aumento della criminalità informatica guidando lo sviluppo digitale del Paese con tecnologie e strumenti avanzati, ma anche competenze adeguate in materia di cybersecurity. Con la stessa ambizione, qualche giorno fa il **Direttore di *ACN*, Roberto Baldoni**, e l'**Amministratore Delegato di *Cisco* Italia, Gianmatteo Manghi** hanno siglato un Protocollo di Intesa, in occasione di un incontro che si è svolto presso la sede del centro di ricerca Cisco Cybersecurity & Privacy Co-Innovation Center a Milano.
(source: https://www.techcompany360.it/accordi/protocollo-di-intesa-tra-cisco-e-lagenzia-per-la-cybersicurezza-nazionale/)

PROTEZIONE DATI PERSONALI E GESTIONE DELLA CYBERSECURITY

24 gennaio – Andrea Lambiase ed Elena Cannone, rispettivamente Chief Digital & Innovation Officer e Data Protection Officer di Axitea, commentano la Relazione Annuale del Garante per la protezione dati personali guardando anche alla gestione delle piattaforme di cybersecurity.
Nella Relazione Annuale presentata a luglio 2022, il Garante per la protezione dei dati personali ha evidenziato che dal 1° gennaio 2021 al successivo 31 dicembre sono state notificate 2.071 violazioni dei dati personali. Comparando la Relazione Annuale con quella del 2021 emerge che rispetto al 2020, dove i casi segnalati erano stati 1.387, vi è stato un **aumento** dei data breach di quasi il doppio. Questo ha reso il 2021 "un anno particolarmente difficile sul fronte della cybersecurity e della protezione dei dati personali".
(source: https://techfromthenet.it/2023/01/24/protezione-dati-personali-e-gestione-della-cybersecurity/)

AL VIA GLI ALLENAMENTI PER LE OLIMPIADI NAZIONALI DI CYBERSECURITY

23 gennaio – È stata inaugurata oggi, in presenza a Torino, **la prima giornata dei Training Camp del Cybersecurity National Lab**: *un'iniziativa rivolta ai giovani ragazzi e ragazze degli istituti superiori* di secondo grado che hanno superato la prima **fase di ammissione di OliCyber, le Olimpiadi nazionali di sicurezza informatica**. Il raduno, primo di tre che si svolgeranno tra gennaio e febbraio in tutta Italia, è la grande novità della terza edizione di OliCyber, che intende offrire a 360 ragazzi l'opportunità di aderire a uno speciale percorso di formazione in vista delle selezioni territoriali che stabiliranno chi può competere alle Olimpiadi vere e proprie, la cui finale si terrà il 27 maggio.
(source: https://www.wired.it/article/cybersecurity-formazione-scuola-olicyber/)

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 dell'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

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

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.