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

Newsletter

ANNO 2022 | N. 11 | DICEMBRE

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 153.800 associati in oltre 188 nazioni (dato aggiornato al 31 agosto 2021) 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

DARKVERSE: IL LATO MALEVOLO DEL METAVERSO E I SUOI RISCHI DI SICUREZZA, PRIVACY E PERCEZIONE

Se cercate una definizione unanime e condivisa di Metaverso, sappiate che non c'è: in compenso ne troverete tante e tutte diverse fra loro. Si spazia da "evoluzione di internet" a "internet delle esperienze", dall'indicazione di "strato digitale multi-vendor, immersivo-interattivo costruito sopra l'internet esistente, cloud distribuito e accessibile da molteplici device" a "una visione hi-tech multimiliardaria immersiva che definirà la prossima era di Internet". Tech Target nella sua guida di approfondimento lo indica come "uno spazio virtuale 3D singolo, condiviso, coinvolgente, persistente in cui gli esseri umani sperimentano la vita in modi che non potrebbero nel mondo fisico". La guida ripercorre la storia del Metaverso, indica gli strumenti di accesso e il suo funzionamento futuro (ovviamente sempre a titolo teorico), specifica le tecnologie abilitanti e il modo in cui è utilizzato oggi, ovvero principalmente per rappresentare avatars e digital twin (gemelli digitali n.d.r.) di persone a mezzo ologrammi, per riunioni in stanze 3D e per scambi di proprietà mediante Non Fungible Tokens (NFT – ovvero Acronimo di Non-Fungible Token (token non fungibili), gli NFT sono una delle applicazioni della finanza decentralizzata: un insieme di servizi e processi che vengono automatizzati grazie all'ausilio di contratti intelligenti (smart contract) e senza la presenza di intermediari.- Fonte Borsa italiana), per vendere e acquistare proprietà immobiliare nel Metaverso o beni digitali disponibili in appositi store virtuali. Nella lista di Pro e contro stilata dal giornalista Mary K. Pratt sono elencati i benefici dell'evoluzione del "nuovo mondo digitale" ma sono anche elencati alcuni pericoli che naturalmente riguardano non solo gli alti costi di accesso alle tecnologie, ma anche aspetti di privacy, di sicurezza e di manipolazione informativa. Naturalmente su questi temi alcuni esperti di sicurezza si sono già espressi.

Ashwin Krishnan (giornalista di security) ha sottolineato come l'attuale mancanza di norme sulla privacy per il Metaverso comporti diverse problematiche: l'errata applicazione e applicabilità delle vigenti normative sulla privacy, come il GDPR; la raccolta di dati invasiva ed estesa; questioni riguardanti i diritti e la proprietà dei dati; la pedopornografia on line; i problemi di privacy da utente a utente.(Fonte Aspetti di privacy del Metaverso).

Gastone Nencini di Trend Micro chiarisce che pur non sapendo esattamente come si svilupperà, è necessario iniziare a pensare oggi a come verrà sfruttato dai cybercriminali al fine di prevenire e proteggere per tempo gli asset digitali. A suo dire: "le Forze dell'Ordine faranno fatica a sorvegliare il Metaverso nei primi anni ed è quindi necessario intervenire oggi, per non rischiare una sorta di Selvaggio West nel mondo digitale". In particolare, il Metaverso malevolo, ribattezzato Darkverse potrebbe assomigliare ad una versione evoluta dell'odierno dark web consentendo ai cybercriminali di coordinare e svolgere attività illegali impunemente. Nei mercati underground che operano nel Darkverse potrebbe essere difficile per la polizia l'attività di infiltrazione a causa dall'assenza di token di autenticazione; infatti, per le comunità criminali chiuse ci sarebbe un ulteriore livello di protezione e di accesso. Questa difficoltà potrebbe fornire la copertura adatta per lo sviluppo di molteplici minacce: dalle frodi finanziarie alle truffe e-commerce, passando per il furto di NFT e per i ransomware. In aggiunta, la natura cyber-fisica del Metaverso potrebbe consentire la compromissione di spazi gestiti dagli operatori di infrastrutture critiche con l'obiettivo di compiere sabotaggi e/o estorsioni di sistemi industriali. Infine, i criminali potrebbero attaccare i dispositivi IoT wearable degli utenti, ovvero le tute interattive, o i device per la Realtà Aumentata (AR) o immersiva, per causare danni fisici. Si potrebbe anche realizzare il cosiddetto "assalto agli avatar"

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

consistente in furti di identità e quindi dell'avatar di un utente similmente a come avviene oggi in internet. In relazione a quest'ultima minaccia, Antonio Madoglio di Fortinet sottolinea i rischi dell'hacking biometrico caratterizzato dal furto dei dati biometrici (impronte digitali, i dati di riconoscimento facciale o le scansioni della retina) dagli apparati di Realtà Aumentata (AR) o Realtà Virtuale (VR) per utilizzarli a fini dannosi di violazione di identità e per commettere frodi, estorsioni, furti con l'identità di qualcun altro. In generale l'avatar di un individuo è essenzialmente un gateway per informazioni di identificazione personale (PII), che restano bersagli primari per gli aggressori. Infatti, poiché gli individui potranno acquistare beni e servizi nelle città virtuali, mediante portafogli digitali, scambi di criptovalute, NFT e qualsiasi valuta utilizzata per effettuare transazioni, gli aggressori digitali avranno una ampia superficie di attacco disponibile per operare. Naturalmente non devono essere esclusi applicazioni, i protocolli e transazioni che all'interno di questi ambienti virtuali saranno tutti possibili bersagli per i criminali.
Alessandro Curioni, Fondatore di DI.GI Academy, specializzato in Information Security & Cybersecurity - Data Protection sottolinea invece i rischi derivanti dalla mancanza di una normazione nel Metaverso (Fonte *Metaverso, i rischi di un mondo nuovo senza leggi e istruzioni per l'uso*). Un primo aspetto è strettamente culturale e riguarda l'avatar e la sua vita. Nei game digitali la morte dell'avatar è accettata come parte del gioco, ma questo cosa significherà nei casi di assassinio dell'avatar nel Metaverso? Quindi i reati che oggi affliggono la persona digitale come dovranno essere regolati nel Metaverso? Avrà senso quindi il backup dell'avatar o la sua "resurrezione"? Altri elementi possono riguardare l'assenza di una normativa di diritto nazionale e internazionale, che rispettivamente inficia sul concetto di proprietà e di sovranità; alla mancanza di questi concetti è legato anche il problema di definire un attacco informativo su una proprietà o su una entità a causa della difficoltà di stabilire chi è il danneggiato, che diritti aveva su quel bene e quindi materialmente in cosa consista il danno alla proprietà. Come potrebbe essere dichiarato un attacco in assenza di una specifica definizione in tal senso? Tutte le domande restano aperte, perlomeno fino ad una appropriata normazione e istituzione di uno statuto giuridico su oggetti e soggetti digitali nel Metaverso.
In ultimo ma non meno importante il rischio concreto e affatto scontato di un aumento della distorsione delle percezioni a causa di disinformazione, deep fake e manipolazione cognitiva e della comunicazione mirata ad influenzare le persone. (o influenza delle masse personalizzata n.d.r.). Rand Waltzman, scienziato informatico presso il RAND Institute (entità di ricerca senza scopo di lucro n.d.r.), ha pubblicato un *lungo approfondimento sui rischi della disinformazione nel Metaverso*, enfatizzando come la manipolazione emotiva e psicologica possa essere accresciuta mediante sistemi di realtà virtuale. L'esperienza di Waltzman deriva da anni di studi su deception (inganno), disinformazione e intelligenza artificiale svolti per circa quattro decenni, inclusi due mandati come program manager presso la Defense Advanced Research Projects Agency (DARPA). I sistemi di VR possono distorcere le percezioni dell'utente che viene tratto in inganno per mezzo dei suoi stessi sensi e questo lo porta ad essere influenzato e indotto a credere anche a informazioni di tipo contraffatto (fake news). Secondo Waltzman non è stata prestata la dovuta attenzione ai social che oggi influenzano le masse, ovvero Facebook, Twitter, Instagram, e tutti gli altri social, se non quando era ormai troppo tardi; ma per la prevenzione di tutti questi fenomeni nel Metaverso potremmo essere in tempo, a patto di far conoscere questi rischi, sviluppare una cultura alla sicurezza digitale e preparare le persone con strumenti di protezione e di difesa preventiva, prima del loro tuffo nel mondo virtuale.

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

VEN 02 DICEMBRE 2022

ORE 15:00-18:30

"SICUREZZA, PRIVACY E INTELLIGENZA ARTIFICIALE"

Algoritmi, intelligenza artificiale, machine learning, trust ed etica: è stato scritto molto sull'argomento, ma quali sono i "fondamentali" da cui partire per affrontare i vari aspetti della relazione tra Sicurezza, Privacy ed Intelligenza Artificiale?
Una volta definita la prospettiva di osservazione, saranno discussi elementi normativi emergenti a livello europeo, identificati impatti del GDPR, e sarà presentata un'ipotesi di ambito di valutazione del rischio – in particolare rispetto alle valutazioni ethics-based. Infine, vedremo come si stanno evolvendo framework e standard per adeguarsi all'era dell'algoritmo.

*Relatrice**: Dott.ssa Francesca Della Mea***
Laureata in Economia Aziendale e Organizzazione presso l'Università Bocconi di Milano, ha maturato un'esperienza di oltre 20 anni in ambito Information Security, prima in Microsoft, poi in Accenture dove ha sviluppato e gestito la practice Accenture Security per l'area IGEM. Successivamente è stata responsabile di practice di consulenza security in aziende specialistiche, gestendo programmi di trasformazione digitale per clienti enterprise (5000-10000 dipendenti). Interessata in particolare a nuovi modelli gestionali per ICT e security, allineamento business-ICT, business security architecture, information risk management, ICT compliance, Security Operations, Security Analytics.
Fa parte del Gruppo di lavoro ISACA Roma su FAIR, dedicato all'analisi quantitative del rischio. È certificata CISM, CISA, CCSK, LBBP (Sigma Lean Black Belt Professional). Ha studiato cinese (HSK4) e si tiene aggiornata sullo scenario asiatico

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.

LE PRINCIPALI NOTIZIE

RISCHI DELLA CYBERSECURITY: LE PREVISIONI DI CROWDSTRIKE DEL 2023

22 dicembre 2022 – Il 2022 sta per concludersi e gli esperti in sicurezza informatica guardano già al *2023* per delineare alcune tra le possibili evoluzioni e tendenze dei rischi della cybersecurity.

CrowdStrike, azienda operante nel settore della sicurezza informatica, individua alcuni trend per il prossimo anno, evidenziando un possibile aumento del numero e della gravità delle violazioni che sfrutteranno in particolare la raccolta di identità.

Nel 2023, gli avversari sfrutteranno gli attacchi basati sull'identità per l'accesso iniziale e il movimento laterale, riducendo il breakout time.

(source: https://www.bitmat.it/blog/sicurezza/rischi-della-cybersecurity-le-previsioni-di-crowdstrike-del-2023/)

CYBERCRIME, ESCALATION DELLE ATTIVITÀ DEI GRUPPI APT AFFILIATI A RUSSIA, COREA DEL NORD, IRAN E CINA. SCARICA IL REPORT

25 dicembre 2022 – Presentato *l'ESET APT Activity Report*, lo studio che ha l'obiettivo di fornire un'analisi periodica sulle attività dei gruppi APT-advanced persistent threat. Nella prima edizione, relativa al T2 2022 (maggio-agosto 2022), i ricercatori non hanno riscontrato alcun calo nell'attività APT svolta da gruppi allineati a Russia, Cina, Iran e Corea del Nord. Anche a più di otto mesi dall'invasione russa, l'Ucraina rimane un obiettivo primario dei gruppi APT vicini alla Russia, come il famigerato Sandworm, ma anche Gamaredon, InvisiMole, Callisto e Turla. L'industria aerospaziale e della difesa, così come le imprese e gli scambi finanziari e in criptovalute, continuano a essere di grande interesse per i gruppi affiliati alla Corea del Nord.

(source: https://www.key4biz.it/cybercrime-escalation-delle-attivita-dei-gruppi-apt-affiliati-a-russia-corea-del-nord-iran-e-cina-scarica-il-report/428774/)

QUELLE "LEGGEREZZE" DELLA PA SULLA PRIVACY CHE PREOCCUPANO IL GARANTE (E TUTTI NOI)

25 dicembre 2022 – Le istruttorie del Garante Privacy sui sistemi di videosorveglianza intelligente nei confronti dei Comuni di Lecce e Arezzo sollevano nuovamente il dibattito sugli eccessi della PA nel fare ricorso alle nuove tecnologie.

Così già era stato per i progetti di "cittadinanza a punti", con l'avvio di istruttorie riguardanti i meccanismi di scoring e premialità nei confronti dei cittadini adottati da alcuni Comuni.

(source: https://www.redhotcyber.com/post/quelle-leggerezze-della-pa-sulla-privacy-che-preoccupano-il-garante-e-tutti-noi/)

CLOUD, CYBERSECURITY E METAVERSO. I TREND TECNOLOGICI DEL 2023

26 dicembre 2022 – L'incertezza economica e il lavoro ibrido guideranno lo sviluppo tecnologico, l'attenzione per la cybersicurezza dovrà essere sempre più alta e il metaverso si farà sempre più a portata di mano.

Ecco i punti i chiave per interpretare il 2023 ed essere preparati a quello che la tecnologia porterà nelle nostre vite lavorative e non.

(source: https://www.key4biz.it/cloud-cybersecurity-e-metaverso-i-trend-tecnologici-del-2023/428343/)

METAVERSO, INCURIOSITI 9 CONSUMATORI SU 10 E PER LE AZIENDE SARÀ MAINSTREAM ENTRO 3 ANNI. IL REPORT

20 dicembre 2022 – Tre quarti dei consumatori che hanno già esperienza *con il metaverso* dichiarano di utilizzarlo e di voler continuare a farlo, evidenziandone il potenziale per le aziende in grado di sfruttare la forza delle esperienze immersive.

Lo rivela il nuovo report dal titolo *"Total Immersion: How Immersive Experiences and the Metaverse Benefit Customer Experience and Operations"*. Lo studio evidenzia come il 77% dei consumatori si aspetta che le esperienze immersive abbiano un impatto sul loro modo di interagire con le persone, i brand e i servizi, mentre sette organizzazioni su dieci ritengono che le esperienze immersive saranno un importante elemento di differenziazione nei rispettivi mercati, in particolare in relazione al customer journey.

(source: https://www.key4biz.it/metaverso-incuriositi-9-consumatori-su-10-e-per-le-aziende-sara-mainstream-entro-3-anni-il-report/429014/)

COOKIE IMPOSTI AGLI UTENTI SUL MOTORE DI RICERCA: IL GARANTE PER LA PRIVACY FRANCESE SANZIONA MICROSOFT PER 60 MILIONI DI EURO SENZA APPLICARE IL GDPR

26 dicembre 2022 – Le norme europee sulla protezione dei dati personali si sono scontrate ancora una volta con un colosso tecnologico statunitense. La Commission Nationale de l'Informatique et des Libertés (CNIL), che è l'autorità per la privacy francese, ha infatti ***sanzionato Microsoft per 60 milioni di euro*** per aver imposto l'installazione di cookie pubblicitari agli utenti di Bing, che è il terzo motore di ricerca più utilizzato al mondo dopo Google e Baidu.

(source: https://www.federprivacy.org/informazione/flash-news/cookie-imposti-agli-utenti-sul-motore-di-ricerca-il-garante-per-la-privacy-francese-sanziona-microsoft-per-60-milioni-di-euro-senza-applicare-il-gdpr)

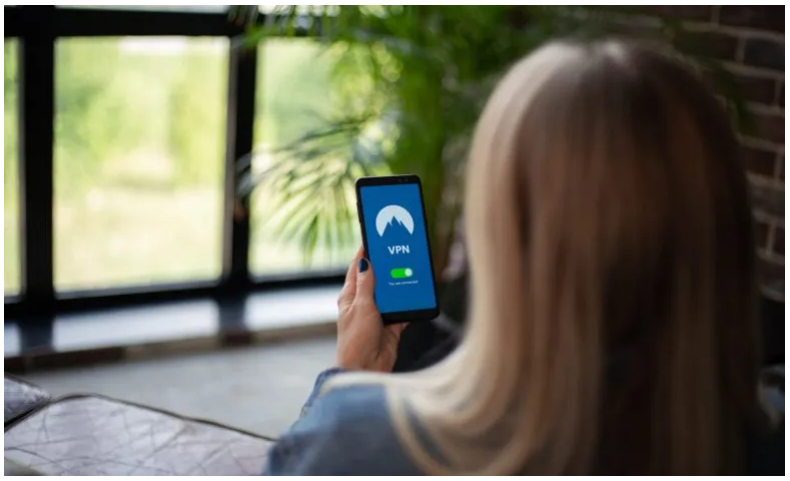
ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

L'AGENZIA PER LA CYBERSICUREZZA SVELA LE TRUFFE PIÙ DIFFUSE SUL WEB

23 dicembre 2022 – L'Agenzia per la Cybersicurezza Nazionale (ACN) ha recentemente pubblicato un *report* che analizza nel dettaglio le principali truffe diffuse sul web. Il Computer Security Incident Response Team, il gruppo di lavoro interno all'Agenzia che ha il compito di monitorare gli incidenti informatici, ha analizzato le principali strategie utilizzate dagli hackers per impossessarsi dei dati sensibili degli utenti, che mettono quindi a rischio la loro identità digitale.
(source: https://www.occhionotizie.it/agenzia-cybersicurezza-svela-truffe-piu-diffuse-web/)

IL GOVERNO DI GIORGIA MELONI HA UN PROBLEMA ENORME CON LA POLITICA DIGITALE, E PER L'ITALIA È UN GROSSO GUAIO

22 dicembre 2022 – Forse si poteva intuire dal primo giorno di governo. Nella lista dei ministri consegnata da Giorgia Meloni al presidente delle Repubblica Sergio Mattarella mancava una casella. Accanto al ministero dell'Innovazione non c'era nessun nome. Anzi. Probabilmente il ministero dedicato alla Trasformazione Digitale non era nemmeno menzionato. Un omissis che è stato corretto in corso d'opera. Alla guida delle politiche digitali è stato messo Alessio Butti, sottosegretario della Presidenza del Consiglio.



Una svista, forse. Ma poi il governo ha cercato di spingere per l'aumento del tetto dei contanti, ha provato a togliere le sanzioni per i commercianti che non accettavano piccoli pagamenti con il Pos, ha proposto di abolire lo Spid per puntare sulla carta di identità elettronica e ha prorogato solo in corner le ricette mediche digitali.
(source: https://www.fanpage.it/innovazione/tecnologia/il-governo-di-giorgia-meloni-ha-un-problema-enorme-con-la-politica-digitale-e-per-litalia-e-un-grosso-guaio/)

INCIDENTI DI SICUREZZA, PERCHÉ FARE UN REPORT È COSÌ IMPORTANTE

21 dicembre 2022 – Oltre al GDPR, sempre più normative, europee o nazionali richiedono la notifica di incidenti cyber. Serve, però, armonizzare i vari obblighi altrimenti si rischia di togliere tempo e risorse alla capacità di difesa. Vediamo cosa prevedono.
(source: https://www.cybersecurity360.it/outlook/incidenti-di-sicurezza-perche-fare-un-report-e-cosi-importante/)

RECONCILING INTERNATIONAL BREACH REPORTING RULES COULD PROVE CHALLENGING

08 dicembre 2022 – Privacy and security chiefs say different countries must sync up rules around cybersecurity incident reporting but contrasting views between governments on how to implement rules could complicate those efforts.
A rash of cyberattacks against critical infrastructure operators, local governments and companies of all sizes in recent years has prompted lawmakers in the U.S., U.K. and European Union to examine when and how cyberattacks should be reported.
(source: https://www.wsj.com/articles/reconciling-international-breach-reporting-rules-could-prove-challenging-11670454175)

MB4.0, IL FUTURO TRA METAVERSO E CYBERSECURITY

22 dicembre 2022 – È necessario diffondere la cultura della sicurezza nel mondo digitale sia a privati che a enti pubblici.
Quella che oggi stiamo vivendo è un'epoca sempre più "phygital", in cui i confini tra fisico e digitale diventano sempre più labili e l'innovazione tecnologica continua ad aprire nuovi scenari e opportunità. In questo contesto, un ruolo centrale è giocato dal concetto di Metaverso, che ci pone davanti a un salto tecnologico in grado di portare un violento scossone nella nostra realtà, digitale eattuale sviluppo tecnologico non solo. Un tema in cui è specializzato Marco Bacini, professore di Marketing Omnichannel presso la facoltà di Economia e management dell'Università Lum di Bari, direttore di diversi master della scuola di Management Lum di Milano e ceo di Mb4.0, agenzia di comunicazione, social media management, influencer marketing, press office, formazione corporate.
(source: https://roma.repubblica.it/dossier-adv/eccellenze-lazio/2022/12/22/news/mb40_il_futuro_tra_metaverso_e_cybersecurity-380243792/)

DENTRO LA NIS 2, PIÙ OBBLIGHI E REGOLE PER LA CYBERSECURITY EUROPEA

20 dicembre 2022 – La **Commissione Europea ha sostituito la direttiva NIS**, il primo atto legislativo a livello dell'UE in materia di cyber sicurezza, **con la Direttiva NIS 2 al fine di rispondere alle crescenti minacce poste dalla digitalizzazione e all'ondata di attacchi informatici e contestualmente rafforzare la sicurezza** in azienda e nelle catene di approvvigionamento, semplificare gli obblighi di comunicazione e introdurre norme più rigorose misure di vigilanza e requisiti di applicazione più severi, comprese sanzioni armonizzate in tutta l'UE.
(source: https://www.cybersecurity360.it/outlook/dentro-la-nis-2-piu-obblighi-e-regole-per-la-cybersecurity-europea/)

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

CISA Certified Information Systems Auditor. An ISACA® Certification

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

CISM Certified Information Security Manager. An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification

CSX-P CSX Cybersecurity Practitioner. An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

ITCA Information Technology Certified Associate An ISACA® Certification

CYBER SECURITY AUDIT An ISACA Certificate

COBIT An ISACA® Framework

CSX CYBERSECURITY NEXUS

IT RISK FUNDAMENTALS An ISACA Certificate

CCAK Certificate of Cloud Auditing Knowledge A Cloud Security Alliance® and ISACA® Credential

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.