ISACA Rome Chapter

Newsletter

ANNO 2023 | N. 5 | MAGGIO

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

CYBER SOLIDARITY ACT: l'Unione Europea "serra le fila" della Difesa

E' datata 18 aprile 2023 la proposta della Commissione Europea chiamata *Cyber Solidarity Act*, che modifica la legge dell'UE sulla cybersicurezza nota come *Cybersecurity Act*). Il Cyber Solidarity Act segna l'ultimo tassello della più ampia strategia di sicurezza informatica dell'UE e la rende operativa, ma certamente il conflitto Russo Ucraino ha accelerato i lavori e a marzo 2022, poco dopo l'invasione russa dell'Ucraina, Bruxelles ha reagito guardando alla guerra come una crescente minaccia di un grave attacco informatico.

L'intento della proposta è rafforzare le capacità di cybersicurezza nell'Ue e in particolare il coordinamento transfrontaliero e pubblico-privato per quanto riguarda l'anticipazione e la lotta agli attacchi informatici. Mira, inoltre, a garantire che tutti i cittadini e le imprese europei siano ben protetti, sia online che offline, promuovendo un ciberspazio aperto, sicuro e stabile. Facile a dirsi, ma certamente non del tutto semplice da implementare. La proposta vuole concretamente rafforzare le capacità nell'UE di individuare, prepararsi e rispondere a minacce e attacchi alla cybersicurezza significativi e su larga scala. A tal fine comprende: **uno scudo europeo per la cybersicurezza**, un **meccanismo globale di emergenza per la cybersicurezza dell'UE legato a individuazione delle vulnerabilità e gestione incidenti.** Ultimo e fondamentale componente è un budget di 1,1 miliardi di euro previsto per l'attuazione.

Il **primo elemento centrale** della proposta sarà **l'istituzione di uno scudo informatico europeo** (Cyber Shield) costituito da centri operativi di sicurezza (SOC) nazionali e transfrontalieri diffusi in tutta l'UE. I diversi centri operativi di sicurezza (SOC) saranno riuniti per integrazione delle diverse piattaforme multinazionali SOC, a loro volta costruite con il sostegno del programma Europa digitale (DEP). Il Cyber Shield avrà il compito di migliorare il rilevamento, l'analisi e la risposta alle minacce informatiche. Nel corso di una prima fase, avviata nel novembre 2022, sono stati selezionati *tre consorzi di centri operativi di sicurezza transfrontalieri* (SOC), che riuniscono organismi pubblici di 17 Stati membri e Islanda, nell'ambito del programma Europa digitale. L'intento è di rendere operativi i SOC nel corso del 2024, creando hub regionali di cooperazione informatica con vicini immediati come i Paesi baltici e il Benelux.

Il **secondo pilastro della legge** si concentra sul potenziamento della capacità di preparazione e risposta alle crisi dell'UE attraverso la **creazione di un meccanismo di emergenza informatica, che verificherà le vulnerabilità in settori critici** come l'energia e i trasporti e fornirà sostegno finanziario per l'assistenza reciproca tra gli Stati membri. È prevista anche la creazione di una "Riserva per la sicurezza informatica" dell'UE composta da società private affidabili e certificate pronte a rispondere a gravi incidenti. Per partecipare a

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

questa Cyber Reserve, le aziende dovranno essere certificate ai sensi di una nuova certificazione della legge sulla sicurezza informatica.

La combinazione di entità pubbliche e private nella proposta (in tema di centri di sicurezza coinvolti per l'allertamento della minaccia n.d.r.) fa eco a un modello già in atto in Ucraina, dove aziende e autorità collaborano per affrontare le minacce informatiche. Certamente questa **commistione fra pubblico e privato ha suscitato un dibattito significativo e l'opposizione della maggioranza degli Stati membri**, specialmente in relazione alla condivisione dell'intelligence e alla qualificazione e responsabilità delle società private coinvolte. Infatti, l'intelligence sulle minacce informatiche può essere sfruttata per violare il sistema informatico di chiunque, sia esso un rivale geopolitico, una rete criminale o un concorrente economico. Si tratta, quindi, di informazioni gelosamente custodite dalle autorità nazionali. Ventiquattro governi europei, hanno invitato Bruxelles a rallentare la sua proposta di Cyber Solidarity per le preoccupazioni legate al mantenimento del potere a livello nazionale in materia di certificazione e dispiegamento di tale riserva. L'attenzione alla cooperazione pubblico-privato deve affrontare anche la concorrenza all'interno dell'architettura istituzionale di Bruxelles, con il braccio diplomatico dell'UE, il Servizio europeo per l'azione esterna (SEAE), che sta attualmente rivedendo il Cyber Diplomacy Toolbox, anch'esso affidato alle imprese private.

Una questione quindi, non di poco conto su diversi fronti.

Un **ulteriore elemento della proposta** è l'istituzione di un **meccanismo di revisione degli incidenti di cybersicurezza**, che esaminerà e analizzerà gli incidenti gravi per migliorare i futuri sviluppi dell'approccio dell'UE alla cyberdifesa. Su richiesta della Commissione o delle autorità nazionali (l'UE-CyCLONe o la rete CSIRT), l'Agenzia dell'UE per la cybersicurezza (ENISA) sarà responsabile del riesame di specifici incidenti di cybersicurezza significativi o su larga scala e dovrebbe presentare una relazione che includa gli insegnamenti tratti e, se del caso, raccomandazioni per migliorare la risposta informatica dell'Unione.

Un punto importante del Cyber solidarity Act riguarda infine, *l'emendamento alla legge sulla sicurezza informatica*, relativo ad **un sistema di certificazione per i "servizi di sicurezza gestiti"** in aggiunta alla certificazione dei prodotti dell'informazione e della tecnologia che sono già coperti dalla legge sulla sicurezza informatica (Cybersecurity Act n.d.r.). Questo perché i servizi di sicurezza gestiti svolgono un ruolo sempre più importante nella prevenzione e mitigazione della sicurezza informatica degli incidenti. La UE ha voluto intervenire contro la possibile frammentazione degli schemi certificativi per evitare che siano adottati schemi incoerenti fra paesi dell'Unione.

In questa fitta rete di entità e autorità ricordiamo anche il neonato *European Cybersecurity Network and Cybersecurity Competence Centre (ECCC)* che mira ad aumentare le capacità e la competitività dell'Europa in materia di cybersicurezza. Collaborerà con una rete di centri nazionali di coordinamento (NCC) per costruire una forte comunità di sicurezza informatica. Con sede a Bucarest, attuerà parti rilevanti dei programmi *Digital Europe* e *Horizon Europe programmes* assegnando sovvenzioni e realizzando appalti.

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.

ISACA
Rome Chapter

EVENTI PASSATI

VENERDÌ 26 MAGGIO 2023
15:00-17:00 (2 CPE)

"GLI SCENARI IN AMBITO IT: STATO DELL'ARTE DI UNO STRUMENTO"

L'obiettivo è stato quello di focalizzare l'attenzione su uno strumento, oggetto di crescente interesse dei principali player che si occupano di norme e best practice, la cui definizione ed utilizzo appare però meno intuitiva e semplice di quanto si potrebbe supporre. Fatto il punto sullo stato dell'arte e confronto sintetico su alcuni approcci.

Relatori:

ing. Alberto Piamonte
Una lunga carriera nel mondo ICT con significative esperienze internazionali, nei laboratori di R&D di primarie aziende internazionali. Istruttore, Implementor ed Assessor COBIT5

Dott.ssa Francesca Della Mea
Ha maturato un'esperienza di oltre 20 anni in ambito Information Security, gestendo programmi di trasformazione digitale per clienti enterprise (5000-10000 dipendenti). È certificata CISM, CISA, CCSK, LBBP,FAIR.

Dott. Glauco Bertocchi
Più di 40 anni di esperienza in IT e nella sicurezza acquisita all'interno di università e istituzioni nazionali. Attivo nella ricerca in ambito protezione e resilienza delle Infrastrutture critiche. Certificato CISM, CDPSE, LA ISO 27001:2013:2022.

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

PROSSIMI EVENTI

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 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>isaca-roma.it

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

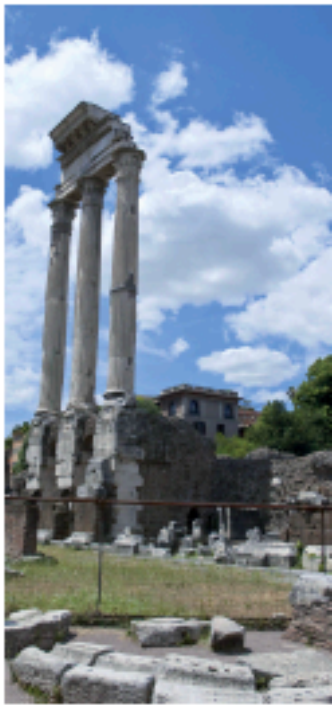
ISACA
Rome Chapter

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

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

ISACA Rome Chapter

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

LE PRINCIPALI NOTIZIE

CYBER SOLIDARITY ACT, COSÌ L'EUROPA DIVENTERÀ RESILIENTE E "SOLIDALE" CONTRO I CYBER ATTACCHI

20 aprile – È stato denominato **EU Cyber Solidarity Act** e creerà "uno scudo europeo per la sicurezza informatica, costituito da centri operativi per la sicurezza interconnessi in tutta l'UE, e un meccanismo di emergenza per la sicurezza informatica completo per migliorare la postura informatica dell'UE".
È questa la ***nuova proposta*** dell'Unione che prevede un **piano di investimenti da 1,1 miliardi di euro** per "rafforzare il rilevamento e la consapevolezza stessa delle minacce e degli incidenti, potenziare la capacità di intervento e rinforzare la solidarietà, il management concertato delle crisi e la capacità di risposta", come si legge dal comunicato ufficiale.
Continuano, dunque, gli sforzi della Commissione Europea per creare **nuove misure atte a contrastare la minaccia cyber**, sempre più incalzante e diventata ormai, soprattutto a seguito dello scoppio della guerra tra Russia e Ucraina, una vera e propria arma, quasi al pari di quelle militari, se non più potente in alcuni casi.
(source: https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-solidarity-act-cosi-leuropa-diventera-resiliente-e-solidale-contro-i-cyber-attacchi/)

EUROPEAN UNION OFFICIALIZES CYBER SOLIDARITY ACT

16 maggio – COn April 18, 2023, the European Commission officialized the launch of the Cyber Solidarity Act. A regulations proposal outlines this European "*cyber shield*", which will be operational in early 2024. The text must now be debated in the European Parliament and Council.
When he spoke at FIC 2023, European Commissioner for the Internal Market, Thierry Breton, compared this project to a "Cyber Galileo". According to him, the Cyber Solidarity Act should allow member States to "*better detect, anticipate and counter significant or large-scale cybersecurity incidents*."
(source: https://incyber.org/en/european-union-officializes-cyber-solidarity-act/)

INTELLIGENZA ARTIFICIALE E CYBERSECURITY: I RISCHI E LE OPPORTUNITÀ PER AZIENDE E AMMINISTRAZIONI PUBBLICHE

23 maggio – *Articolo di **Greta Nasi**, docente di Amministrazione pubblica e direttore del Master of science in cyber risk strategy and governance dell'Università Bocconi*
La pervasività delle tecnologie nella vita quotidiana di cittadini e aziende rende più vulnerabili i sistemi informatici ed espone ad innumerevoli rischi. **I dati pubblicati nel** *rapporto Clusit 2023* evidenziano un incremento significativo degli attacchi verso tutte le tipologie di aziende, ma in particolare verso le amministrazioni pubbliche, le aziende manifatturiere, i servizi professionali e il comparto informatico.
A fronte di attacchi cyber sempre più frequenti e con conseguenze critiche in circa l'80% dei casi per le vittime a livello di reputazione, di impatto economico, sociale e dal punto di vista geopolitico, **servono contromisure e strumenti adeguati** che non sono sempre disponibili nelle aziende ed istituzioni italiane.
(source: https://forbes.it/2023/05/23/intelligenza-artificiale-cybersecurity-rischi-opportunita/)

UE: GDPR COMPIE 5 ANNI, SANZIONI PER VIOLAZIONI DELLA PRIVACY PARI A 5 MILIARDI DI EURO

24 maggio – Il 25 maggio di 5 anni fa entrava definitivamente in vigore il Regolamento europeo sulla protezione dei dati personali, segnando una svolta storica con l'introduzione di un'unica normativa valida per tutti i 27 Paesi dell'Unione europea.
Secondo l'Osservatorio di Federprivacy, da allora a oggi le autoritá di controllo dello Spazio Economico Europeo hanno irrogato ben 5 miliardi di euro di sanzioni per violazioni della privacy, ma i problemi sono tutt'altro che risolti. Anche se nel 2018 quello che è poi divenuto noto come Gdpr introdusse una disciplina all'epoca innovativa basata sul principio di "responsabilizzazione" (accountability), che richiedeva alle imprese pubbliche e private l'adozione di comportamenti proattivi per essere in grado di dimostrare la concreta adozione delle misure di sicurezza necessarie a garantire il rispetto del Regolamento Ue, da allora la tecnologia si è evoluta in modo talmente rapido da rendere sempre piú complessa la tutela della privacy dei cittadini, con preoccupanti impatti sulle loro stesse vite che sono divenuti progressivamente evidenti, spiega una nota.
(source: https://www.italiaoggi.it/news/ue-gdpr-compie-5-anni-sanzioni-per-violazioni-della-privacy-pari-a-5-miliardi-di-euro-202305241207087548)

BILL GATES METTE IN GUARDIA ANCHE COLOSSI COME GOOGLE E AMAZON DALL'INTELLIGENZA ARTIFICIALE

23 maggio – L'*intelligenza artificiale* è destinata a rivoluzionare il rapporto tra uomo e *digitale* così come lo conosciamo e a mettere in crisi anche aziende strutturate come *Google* e *Amazon*. Parola di Bill Gates, che il 22 maggio, nel corso di un evento organizzato da Goldman Sachs e SV Angel proprio sulla tecnologia del momento, ha individuato quale potrebbe essere il prodotto in grado di dare all'azienda che lo realizzerà un netto vantaggio su tutte le altre.

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

Come *riporta Il Sole 24 Ore*, secondo il fondatore di *Microsoft* arriverà presto uno "*sconvolgimento epocale*" capace di modificare nel profondo i comportamenti quotidiani degli utenti: "*Chiunque realizzerà per primo un agente personale*" dotato di intelligenza artificiale, riuscirà a far sì che "*nessuno consulti più motori di ricerca, siti di produttività o Amazon*". In particolare, Gates immagina un assistente virtuale capace di studiare e comprendere a fondo le necessità e le abitudini di navigazione e acquisto delle persone, per poi utilizzarle per aiutarle a "*leggere le cose che non hanno tempo di leggere*".
(source: https://www.wired.it/article/intelligenza-artificiale-bill-gates-google-amazon/)

PA & CYBERSECURITY/ COSÌ LA SNA PREPARA DIRIGENTI E FUNZIONARI PUBBLICI

28 maggio – La Scuola Nazionale dell'Amministrazione (SNA) è un'istituzione di selezione, reclutamento e formazione professionale dei dirigenti e funzionari della pubblica amministrazione (PA) la quale dipende funzionalmente dalla Presidenza del Consiglio dei Ministri (PCM). È recente l'iniziativa svolta dalla SNA nel campo della cyber sicurezza della PA, rivolta ai vertici delle amministrazioni pubbliche centrali: PCM, Ministeri, Inps, Inail, Istat, Agenzia delle Entrate, Agenzia delle Dogane e dei Monopoli, Organi costituzionali. Tale attività formativa si è concretizzata nella summer school, svoltasi dal 12 al 14 luglio 2022 a Roma, d'intesa con l'Agenzia per la cybersicurezza nazionale (ACN). Riguardo a tali attività formative, è stato intervistato il Professor Remo Morzenti Pellegrini, Vicepresidente della SNA. Questa è l'ultima di una serie di interviste che trattano differenti aspetti correlati alla cybersicurezza, disinformazione e intelligence.

(source: https://www.ilsussidiario.net/news/pa-cybersecurity-cosi-la-sna-prepara-dirigenti-e-funzionari-pubblici/2543689/)

ChatGPT POTREBBE LASCIARE L'EUROPA PER NON AVER RISPETTATO IL GDPR

28 maggio – Da qualche mese, molte voci si sono levate per avvertire dei **potenziali pericoli che l'IA rappresenta per il futuro dell'umanità**. Alcuni di loro sono anche attori importanti in questo settore vivace.
Geoffrey Hinton, considerato uno dei padri fondatori dell'AI, ha appena lasciato Google per dare l'allarme. Ancora più sorprendentemente, il 24 maggio 2023, anche il capo di OpenAI ha preso posizione invitando i governi a istituire un sistema di regolamentazione. Piuttosto encomiabile dal leader dell'azienda **dietro ChatGPT.**
(source: https://cybeout.com/2023/05/chatgpt-potrebbe-lasciare-leuropa-per-non-aver-rispettato-il-gdpr/)

CYBERCRIME, 27 CAMPAGNE CONTRO L'ITALIA LA SCORSA SETTIMANA

29 maggio – L'Italia è stata presa di mira da 27 campagne del cybercrime la scorsa settimana. Gli esperti di cybersecurity di CERT-AgID hanno rilevato 6 malware: Strela, AgentTesla, Amadey, Quakbot, Ursnif e Lokibot. Massiccio phishing sulle banche.
(source: https://www.difesaesicurezza.com/cyber/cybercrime-27-campagne-contro-italia-la-scorsa-settimana-2/)

COME STA PROCEDENDO LA STORIA DEL CLOUD DELLA PUBBLICA AMMINISTRAZIONE

28 maggio – La digitalizzazione dell'Italia è una delle spese più onerose inserite all'interno delle varie missioni del PNRR. Circa 50 miliardi di euro sono stati destinati alle opere – comprese le infrastrutture – da realizzare per consentire al nostro Paese di rimettersi al passo con i tempi, colmando quel gap con altri Stati che da anni si sono "convertiti" al digitale. Fondamentale sarà il completamento della transizione al cloud della Pubblica Amministrazione, con la gestione che lo scorso 19 gennaio è passata dall'AgID (Agenzia per l'Italia digitale) all'ACN.
(source: https://www.giornalettismo.com/cloud-pubblica-amministrazione-a-che-punto-siamo/)

CYBERSICUREZZA. TOFALO: IMPORTANTI PASSI AVANTI NEGLI ULTIMI ANNI. PER IL FUTURO OCCORRE UNA MAGGIORE DIFFUSIONE DELLA "CULTURA INFORMATICA"

24 maggio – In occasione dell'Expo Security & Cyber Security Forum di Pescara, *Report Difesa* ha avuto modo di intervistare l'Ing. Angelo Tofalo, già sottosegretario alla Difesa nei governi Conte I e Conte II, con cui ci si è brevemente soffermati sui maggiori rischi attualmente presenti nel mondo cibernetico e sulle varie iniziative intraprese dai nostri governi e dalla nostra Pubblica Amministrazione al fine di salvaguardare le proprie funzioni e il tessuto produttivo del Paese.
(source: https://www.reportdifesa.it/cybersicurezza-tofalo-importanti-passi-avanti-negli-ultimi-anni-per-il-futuro-occorre-una-maggiore-diffusione-della-cultura-informatica/)

LE FIGURE NELLA CYBERSECURITY: QUALI SONO QUELLE PIÙ RICERCATE?

24 maggio – La cybersecurity è diventata un tema di estrema importanza nell'era digitale in cui viviamo.
Le minacce informatiche sono sempre più frequenti e sofisticate, mettendo a rischio la sicurezza dei sistemi aziendali e dei dati sensibili.
In questo contesto, è fondamentale comprendere quali sono le figure più ricercate nel settore della cybersecurity e quali competenze sono richieste dal mercato oggi.
Inoltre, è importante capire quali investimenti a lungo termine sono necessari per proteggere le aziende da queste minacce sempre in evoluzione.
(source: https://www.tag24.it/637403-figure-nella-cybersecurity/)

CYBERSECURITY, PER LE PMI PIÙ EFFICACE UNA GESTIONE "ESTERNA"

25 maggio – **Una complessa soluzione di cybersecurity non garantisce la protezione migliore senza la gestione da parte**

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

ISACA
Rome Chapter

di uno specialista competente. Per le aziende, d'altro canto la ricerca di specialisti della sicurezza è complicata dal fatto che, a livello globale, ci sono pochi esperti in questo settore. Il dato è stato quantificato da (Isc)², che nel suo 2022 Cybersecurity Workforce Study ha segnalato un gap di competenze di 3,4 milioni di lavoratori nel mercato professionale. Questa situazione ha portato le aziende ad affidare alcune funzioni IT ai Managed Service Provider (Msp) o Managed Security Service Provider (Mssp), per assicurarsi le competenze necessarie e avere team aggiornati.

(source: https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-per-le-pmi-piu-efficace-una-gestione-esterna/)

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

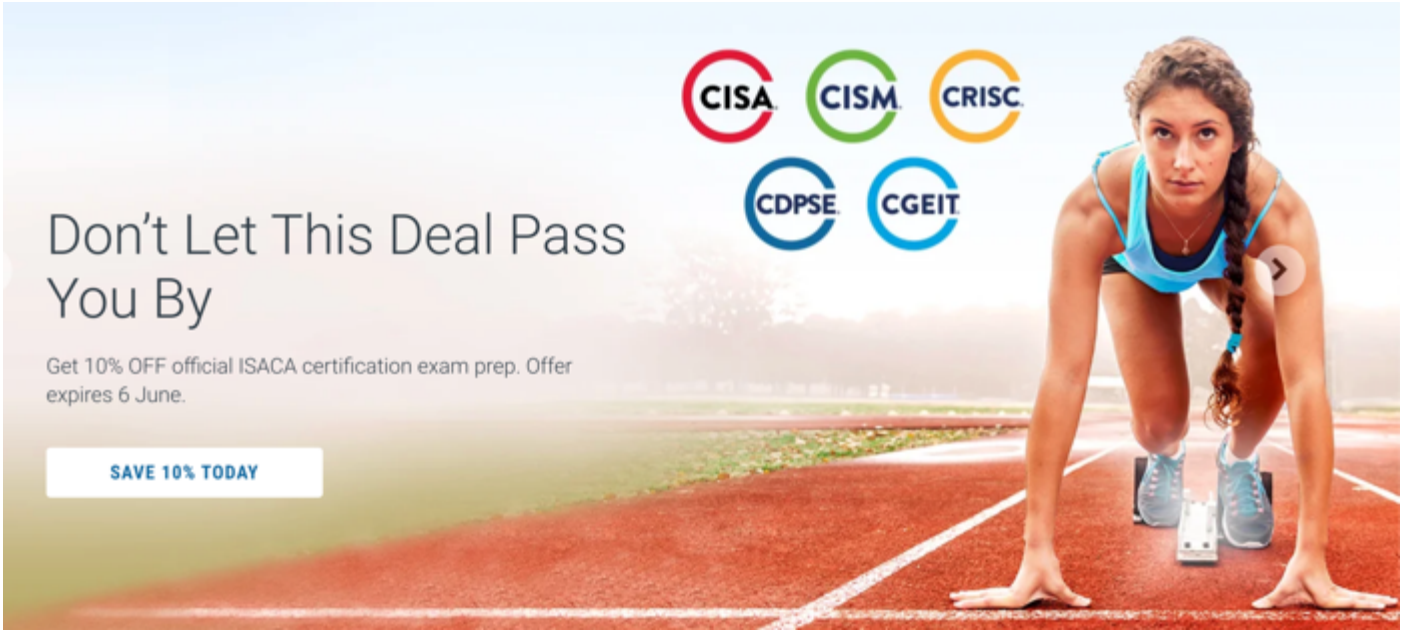
http://www.isacaroma.it/

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.



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

ISACA
Rome Chapter

GET CERTIFIED

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/*

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.