ISACA Rome Chapter

Newsletter

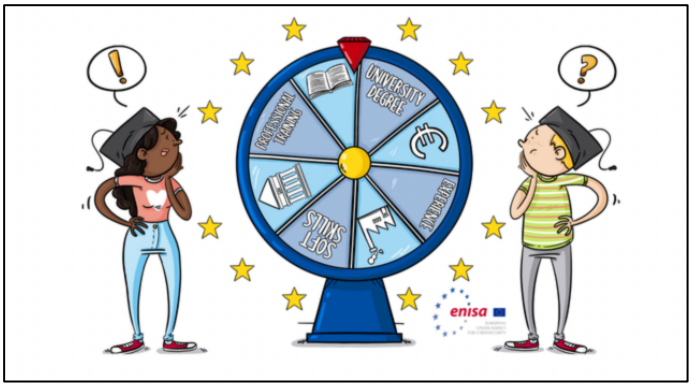
ANNO 2023 | N. 4 | APRILE

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

L'European Cybersecurity Skills Framework basta per risolvere il Cyber Skill gap?



Si chiama European Cybersecurity Skills Framework (ECSF) ma si pronuncia "classificazione delle competenze di Cybersecurity". Per tutti coloro che credevano di non averne bisogno, l'Europa ha risposto che invece serviva, perché nel 2023 proclamato anno europeo delle competenze, la questione del Cyber Skill gap (la difficoltà di trovare professionisti e risorse in questo ambito lavorativo, n.d.r.) è un problema serio e giudicato significativo date le sfide da risolvere nate con la pandemia e aumentate dalla Guerra Russo/Ucraina. Certo il Cyber skill gap ha più di una causa e quella che viene indirizzata dal Framework risolve solo in parte il problema dei profili di Cybersecurity che non si trovano. Ma andiamo con ordine: capiamo cosa sia il Framework e cosa punti a risolvere. Per i restanti problemi aperti vi fornirò uno spunto di riflessione.

L'ECSF fornisce uno strumento europeo aperto per costruire una comprensione comune dei profili dei ruoli professionali della sicurezza informatica e mappature comuni con le abilità e le competenze appropriate richieste. In pratica è un tool che vuole essere di uso tangibile per chi abbia la necessità di identificare l'articolazione di compiti, competenze, abilità e conoscenze associate ai ruoli dei professionisti europei della sicurezza informatica. Al di là dei molteplici job names che potreste trovare su Linkedin e che spesso rendono complicata (soprattutto ai non addetti ai lavori) la comprensione di "quale figura sia in relazione con quale attività professionale", l'ECSF classifica 12 profili, che vengono singolarmente analizzati nel dettaglio delle corrispondenti responsabilità, competenze, sinergie e interdipendenze permettendo la comprensione dei ruoli e facilitare il riconoscimento dei bisogni professionali in materia di cybersicurezza per ogni tipo di progetto tecnologico che si possa avere ed in cui sia necessario coprire la componente di sicurezza informatica. I profili sono: Chief Information Security Officer (CISO), Cyber incident Responder, Cyber Legal Policy and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensic Investigator, Penetration Tester.

Il framework è racchiuso in un documento e completato da un manuale utente, che costituisce una guida pratica al suo utilizzo, basata su esempi e casi d'uso in sette organizzazioni che già usano l'ECSF in diversi contesti. Per chi fosse interessato ad approfondire sono anche disponibili tre webinar sull'argomento: ***The principles, the vision, the structure and the benefits of the ECSF***, ***Assessing Cyber Skills on the basis of the ECSF***, ***Take a walk on the CISO side***.

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

Per gestire la governance, attuazione ed evoluzione dell'ECSF è stato istituito un Ad-Hoc Working Group (AHWG) per assistere l'ENISA a lavorare con le comunità dell'UE e allineare le competenze dei professionisti di sicurezza informatica con l'ECSF in modo progressivo agli sviluppi tecnologici e alle relative competenze necessarie.

Il motivo per cui L'UE abbia deciso di fornire una guida alle professioni di sicurezza informatica è stato chiarito da Despina Spanou, capo di gabinetto del vicepresidente Margaritis Schinas, della Commissione europea, che ha dichiarato: *"dobbiamo assicurarci di affrontare quella che potrebbe diventare la nostra più grande sfida: come avere le persone giuste con le giuste competenze per proteggere i nostri cittadini e le nostre economie da attacchi informatici sempre più pervasivi in tutti i settori critici…(omissis)… Il quadro europeo delle competenze in materia di cybersicurezza sarà uno strumento tangibile per aiutare a identificare i profili di posti di lavoro che sono il più necessario sul campo. Può diventare un fattore abilitante per un linguaggio europeo comune sulle competenze in materia di cybersicurezza nell'intero ecosistema cibernetico europeo e un elemento fondamentale per il lavoro della Commissione su un'autentica accademia delle competenze in materia di cybersicurezza"*. Questo intervento che, oltre a risolvere il Cyber skill gap, mira ad aumentare le capacità di protezione dei nostri asset digitali europei, ha anche di fatto annunciato la nascita di una accademia Europea, la Cybersecurity Skills Academy, come iniziativa non legislativa, nell'ambito della priorità strategica "*Promuovere il nostro stile di vita europeo*", una delle 6 priorità della commissione europea per il quinquennio 2019-2024 nell'ambito della *strategia e politica europea*.

Come corollario dell'iniziativa Europea, per orientare i ragazzi verso studi Europei di Cybersecurity è stato reso disponibile il *CyberHEAD, un database di 137 programmi in 26 paesi dell'Unione* per studiare la Cybersecurity a livello di università. L'Italia è presente con 17 corsi di studi, nelle maggiori città.

Per completare il quadro delle cause del Cyber skill gap e fedelmente a quanto annunciato nella premessa, vi condivido i risultati della mia esperienza diretta sul mercato nel lasso degli ultimi 26 anni: sicuramente spiegare il "chi fa cosa" nella Cybersecurity aiuta le aziende a capire di quali figure abbiano bisogno per coprire esigenze professionali di sicurezza informatica. Ma se pensate che il problema sia solo tutto qui, forse dovreste allargare la visuale: il problema del Cyber skill-gap è solo in parte correlato alle professionalità e alle correlate definizioni e competenze. Infatti, i motivi per cui non si trovano risorse in questo campo risiedono in altri aspetti che ragazzi e ragazze neolaureate o professionisti competenti cercano e che spesso non trovano:

1. Le offerte condizioni economiche e benefit possono non essere appropriati e commisurate al ruolo richiesto, solitamente sono sottostimate con le scuse più improbabili e con prospettive di carriera da "miraggio nel deserto".
2. Le job description raramente si concentrano su un solo ruolo ma pretendono di includere più di un ruolo specialistico sotto lo stesso job title tentando di gabbare il candidato e offrendo un solo stipendio medio per i diversi profili-in-uno richiesti.
3. I candidati/e vogliono conoscere i valori dell'azienda per "sposare un progetto" e cercano informazioni per la natura dell'azienda e sulla sua cultura lavorativa per capire se dovranno "vivere per lavorare" invece che "lavorare per vivere" come vorrebbero. Spesso queste informazioni non sono minimamente fornite.
4. Le aziende non si formano abbastanza per seguire le evoluzioni professionali del mercato del lavoro ed anche i responsabili HR restano spesso indietro nelle professionalità tecnologiche dell'ICT e della Cybersecurity.
5. Infine le famiglie non incitano i propri figli e soprattutto le ragazze ad abbracciare discipline STEM fin dalle scelte delle scuole superiori.

Come si risolvono questi elementi? Per i punti da 1 a 4, in aggiunta a misure esplicative come l'ECSF, è opportuno attuare una politica di talent management più accurata e centrata sulle persone, attuando politiche in favore delle "risorse" umane (se sono risorse allora dovrebbero essere trattate come tali e non come numeri secondo le logiche di "la persona costa" o "la persona è utile ma non indispensabile").

Per il punto 5 è probabilmente necessario includere maggiormente le famiglie nei percorsi di orientamento agli studi per allargare la visuale anche a loro.

Lo skill-gap si può risolvere e l'ECSF è un importante passo in avanti, ma la soluzione finale comporterà interventi culturali a vari livelli sociali per supportare il

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

cambiamento della transizione digitale e facilitare una adeguata e appropriata uguale transizione sociale. O almeno questo è il mio augurio.

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!

EVENTI PASSATI

VENERDÌ 24 MARZO 2023
15:00-17:00 (2 CPE)

"L'IMPORTANZA DELLA FORMAZIONE NELLA PROTEZIONE DEI DATI PERSONALI. Un esempio di formazione per la filiale bancaria"

L'obbligo di formazione (artt. 29 e 32 del GDPR) delle persone autorizzate al trattamento riveste, come peraltro nella previgente normativa, grande importanza nella protezione dei dati personali ed è posta oggi anche sotto la sorveglianza del DPO [art. 39 c. 1 lettera b) del GDPR]. Appare però necessario che tale formazione verta in particolar modo sui trattamenti effettivamente svolti dalle diverse unità organizzative in cui è articolata l'azienda. Si presenta un esempio di seminario orientato al personale che opera in una filiale bancaria.
Indice dell'intervento:

1. Importanza della formazione nella data protection: gli obblighi derivanti dal GDPR e da altri provvedimenti del Garante privacy.
2. Il ruolo del DPO e la relazione con la formazione sulla cybersecurity .
3. Un esempio concreto: la formazione per una filiale bancaria
   a) Inquadramento normativo e definizioni
   b) I principali adempimenti svolti in filiale: resa della informativa e raccolta del consenso.
   c) Problematiche connesse: esercizio dei diritti da parte della clientela, marketing, accesso a dati bancari della clientela, disciplina delle comunicazioni alla clientela .

*Relatore: **Dott. Cesare Maria De Santis Puzzonia***
Ha lavorato per diverse aziende ed Enti - Ispettorato Telecomunicazioni e Assistenza al Volo dell'A.M., Ispettorato Logistico dell'A.M., Banca Nazionale del Lavoro, Ipacri SpA (Club sul Computer Crime), Istinform SpA, Euros Consulting SpA ed OASI SpA - prima di intraprendere un autonomo percorso professionale. Attualmente è amministratore unico di PRIMAe srl, società di consulenza operante sul tema della protezione dei dati personali ed è in possesso della certificazione CISM (Certified Information Security Manger) di ISACA ed iscritto altresì nel registro "Data Protection Officer", in accordo alla norma UNI 11697:2017, di KHC. Tra i clienti di PRIMAe srl si annoverano diverse società finanziarie e banche in alcune delle quali svolge il servizio DPO.

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

ISACA
Rome Chapter

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

LE PRINCIPALI NOTIZIE

LE HARD SKILL CHE SERVONO PER LAVORARE NELLA CYBER SECURITY

26 aprile – Se le minacce alla sicurezza informatica possono essere un problema per qualsiasi organizzazione che deve proteggere dati digitali, asset e reputazione aziendale, allora la soluzione è dotarsi di persone con competenze appropriate alla sfida. Le competenze ICT e di cyber security più richieste e/o più adatte a colmare tale gap, sono ricomprese in tre categorie di competenze: **competenze tecniche in primis, cosiddette hard skill**, che coprano i temi dell'ICT e le basi della sicurezza informatica; **le competenze trasversali come seconda priorità genericamente note come soft skill**, che possono ricomprendere la capacità di leadership, il team working, il problem solving etc; infine **la terza competenza è l'esperienza, ovvero la capacità di saper usare insieme le soft e hard skills**.
Per acquisire tutte e tre le categorie di competenze, i master tecnici in cyber security assolvono pienamente alla preparazione sulle hard skill e grazie al mezzo del tirocinio consentono ai discenti di affinare anche i soft skill mettendo in pratica quanto imparato in team, mediante gaming ed esercitazioni pratiche.
(source: https://www.cybersecurity360.it/outlook/le-hard-skill-che-servono-per-lavorare-nella-cyber-security/)

FRATTASI: "LA CYBERSICUREZZA È TRASVERSALE, STRATEGICO FARE SISTEMA"

20 aprile – Cybersicurezza non vuol dire solo crimine informatico, ma è un concetto trasversale che si applica a ogni attività umana e ai servizi civili, dal settore bancario a quello della salute o dei trasporti. A dirlo è stato il Pref. Bruno Frattasi, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, intervenuto il 18 aprile a Roma in apertura della cerimonia di premiazione dei vincitori di Cyber X Mind4Future, il programma di formazione sui temi della sicurezza cibernetica ideato da Leonardo e Cyber4.0, Centro di competenza nazionale promosso dal Ministero delle Imprese e del Made in Italy. "La cybersicurezza è un tema che tocca tutti indistintamente - ha detto il Direttore Generale di ACN - per questo bisogna 'mettere insieme il mondo della sicurezza con il mondo delle imprese e questi due mondi si devono parlare. Possiamo fare qualcosa di buono solo insieme".
(source: https://www.acn.gov.it/notizie/contenuti/frattasi-la-cybersicurezza-e-trasversale-strategico-fare-sistema)

CYBER: TOWARDS STRONGER EU CAPABILITIES FOR EFFECTIVE OPERATIONAL COOPERATION, SOLIDARITY AND RESILIENCE

18 aprile – Today, the Commission has adopted a proposal for the **EU Cyber Solidarity Act** to strengthen cybersecurity capacities in the EU. It will support detection and awareness of cybersecurity threats and incidents, bolster preparedness of critical entities, as well as reinforce solidarity, concerted crisis management and response capabilities across Member States. The Cyber Solidarity Act establishes EU capabilities to make Europe more resilient and reactive in front of cyber threats, while strengthening existing cooperation mechanism. It will contribute to ensuring a safe and secure digital landscape for citizens and businesses and to protecting critical entities and essential services, such as hospitals and public utilities.
(source: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243)

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

I NUOVI CONTRATTI DI SPID ARRIVANO A GIUGNO

20 aprile – A suggellare la **pace tra il *governo Meloni* e i gestori di *Spid*,** il sistema pubblico di identità digitale, ci sono i **40 milioni di euro allocati** nel decreto del *Piano nazionale di ripresa e resilienza (Pnrr),* fresco di fiducia dell'esecutivo alla Camera. E tanto basta per mettere al riparo **Spid dalla scadenza delle convenzioni dei gestori,** che l'Agenzia per l'*Italia* digitale (Agid) aveva prorogato d'ufficio da fine 2022 al **prossimo 23 aprile** per non lasciare scoperto il servizio.
(source: https://www.wired.it/article/spid-nuovi-contratti-giugno-gestori-governo-durata/)

MICROSOFT VUOLE COINVOLGERE PIÙ DONNE NEL CAMPO DELLA SICUREZZA INFORMATICA

25 aprile – **Microsoft** ha deciso di investire nel miglioramento delle competenze dei nuovi dipendenti nel campo della **sicurezza informatica**, in particolare per le **donne** e perlopiù provenienti da **Sud America e Asia**. **Più donne nella sicurezza informatica: con Microsoft è possibile**

Argentina, Cile, Indonesia e Spagna fanno parte degli attuali 28 paesi coperti dalla **Cybersecurity Skills Initiative**, il cui scopo è fornire sovvenzioni e opportunità di finanziamento a organizzazioni non profit e altri istituti scolastici per contribuire a fornire più formazione.
Questo è quanto affermato da Microsoft: le donne costituiscono solo un quarto della forza lavoro della sicurezza informatica. E non solo. L'azienda fa presente il suo **impegno nei confronti delle "popolazioni storicamente sottorappresentate"**.
(source: https://techprincess.it/microsoft-donne-sicurezza-informatica/)

LE MIGLIORI RISORSE ONLINE PER OTTENERE IL MASSIMO DALL'INTELLIGENZA ARTIFICIALE

25 aprile – La recente ondata di servizi di **intelligenza artificiale** generativa, da **ChatGpt** a **Midjourney**, è progettata per essere semplice da usare: l'idea è che chiunque possa sfruttare questi sistemi per produrre testo o immagini ricorrendo a un linguaggio naturale e non tecnico.
Tuttavia, c'è ancora molto da imparare su *come ottenere il massimo da questi strumenti* e sulla tecnologia su cui si poggiano, soprattutto se l'obiettivo è utilizzarli per fare qualcosa di veramente creativo. Dedicando un po' di tempo alle risorse che vi proponiamo qui sotto, sarete in grado di **padroneggiare l'Ai in modo più efficace rispetto all'utente medio**.
(source: https://www.wired.it/article/intelligenza-artificiale-migliori-risorse-online/)

IL FENOMENO CHATGPT E COME MITIGARE I RISCHI DI SICUREZZA

24 aprile – Il fenomeno ***ChatGPT*** è entrato a fare parte della nostra esperienza privata e lavorativa. Ma quali sono le implicazioni in ambito sicurezza e come attivare una strategia di protezione realmente efficace?
Secondo **Cyber Guru**, società italiana che offre programmi di formazione per la security awareness, le persone sono la prima e più importante barriera difensiva di un'organizzazione. Se l'intelligenza generativa permette agli hacker di perpetrare attacchi più numerosi e sofisticati, l'adozione di comportamenti corretti e consapevoli è l'arma più potente a disposizione delle aziende. Per sconfiggere il nemico e mitigare i rischi, occorre attivare quindi un percorso di apprendimento permanente rivolto all'intera popolazione aziendale, come spiegano i manager della società.
(source: https://www.cybersecurity360.it/nuove-minacce/il-fenomeno-chatgpt-e-come-mitigare-i-rischi-di-sicurezza/)

ALLINEARE LA SICUREZZA AL BUSINESS PER RAGGIUNGERE GLI OBIETTIVI AZIENDALI

18 aprile – Uno dei principali errori commessi dalle imprese è **pensare alla cybersecurity in maniera reattiva e non allineata agli obiettivi di business**; *l'ultima indagine di Forrester Consulting per conto di WithSecure* ha evidenziato questa problematica e spiegato come la sicurezza orientata al business possa portare benefici effettivi alle aziende.
L'approccio, al contrario dei metodi tradizionali che si focalizzano sulle minacce tradizionali o sul rendimento degli investimenti in cybersecurity, è pensato per **semplificare le attività di sicurezza occupandosi solo di quelle che assicurano il raggiungimento degli obiettivi di business.**
(source: https://www.securityinfo.it/2023/04/18/imprese-sicurezza-obiettivi-business/)

SICUREZZA, COSÌ IL GOVERNO CINESE PENETRA NELLA TECNOLOGIA USA

20 aprile – **Il Governo cinese sta penetrando negli ecosistemi tecnologici statali degli Stati Uniti**". Inizia con questo monito un recente rapporto pubblicato da ***China Tech Threat***, un centro di ricerca americano specializzato nell'analisi delle "minacce alla sicurezza nazionale derivanti dalle partnership delle società tecnologiche di Pechino con l'esercito cinese", dal titolo: "States of denial vs. States of momentum: dangerous Chinese technology in US State Government systems and rising efforts to prohibit contracts supplying it".
(source: https://www.agendadigitale.eu/sicurezza/la-penetrazione-del-governo-cinese-negli-ecosistemi-tecnologici-statunitensi/)

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

CYBERSICUREZZA, SALGONO GLI ATTACCHI RANSOMWARE MA LA METÀ DELLE AZIENDE NON HA DIFESE

18 aprile – Continua a salire la minaccia degli **attacchi ransomware** alla cybersecurity a livello globale. A dirlo è il Rapporto Annuale sulle Minacce Informatiche pubblicato oggi, 18 aprile, da **Thales** e condotto su circa 3 mila professionisti IT provenienti da organizzazioni pubbliche e private di 18 diversi paesi, tra cui l'Italia.

Circa la metà dei professionisti (47%) ritiene che le minacce alla sicurezza stiano aumentando in volume o gravità e quasi uno su due (48%) segnala un incremento degli attacchi ransomware. Il 51% delle aziende, però, non dispone di un piano formale per proteggersi da questa tipologia di attacchi.

(source: https://www.milanofinanza.it/news/cybersicurezza-salgono-gli-attacchi-ransomware-ma-la-meta-delle-aziende-non-ha-una-difesa-202304181947504021)

TIM CRESCE SUL MERCATO DELLA CYBERSICUREZZA

21 aprile – **Tim** cresce sul mercato della cybersecurity e acquisisce Ts-Way, azienda italiana specializzata nei servizi di prevenzione e analisi degli attacchi informatici (cyber threat intelligence). L'operazione è stata perfezionata attraverso Telsy, società del Gruppo focalizzata nel settore della cybersecurity, che opera nell'ambito di Tim Enterprise.

L'iniziativa valorizza e completa il portafoglio di soluzioni di cybersecurity a sostegno delle grandi aziende e della Pubblica amministrazione e rappresenta un'ulteriore tappa nel consolidamento della leadership di Tim Enterprise come piattaforma Ict più grande d'Italia nella cybersecurity, IoT e cloud. "Con questa operazione cresciamo ulteriormente sul mercato della cybersecurity e rafforziamo le nostre competenze per gestire anche i rischi cyber più complessi", ha commentato **Eugenio Santagata**, Chief Public Affairs & Security Officer di Tim e Amministratore delegato di Telsy.

(source: https://www.agenzianova.com/news/tim-cresce-sul-mercato-della-cybersicurezza/)

LEONARDO PER IL FUTURO DEI PORTI E LA CYBERSECURITY CON ADSP

21 aprile – Si è tenuto ieri presso Palazzo Biscari, a Catania, il convegno "*Digitalizzazione e cybersecurity - Connubio imprescindibile per i porti, infrastrutture strategiche e critiche del sistema Paese*", organizzato dall'*Autorità di sistema portuale (AdSP) del Mare di Sicilia Orientale* in partnership con Leonardo. La giornata è stata l'occasione per un confronto con istituzioni europee e nazionali su quelle che sono le esigenze attuali e future di un porto, in termini di digitalizzazione, d sicurezza ed efficienza. Ai lavori hanno partecipato esponenti della **Commissione europea**, del **Governo** e di **RAM (Rete Autostrade Mediterranee)**, società in house del **Ministero delle Infrastrutture e dei Trasporti** nonché soggetto attuatore per la gestione e implementazione della **Piattaforma Logistica digitale Nazionale** (PLN). *(source: https://www.redhotcyber.com/post/la-potenza-di-gpt-4-lai-di-microsoft-sta-per-sorprenderci-con-un-super-computer-di-ultima-generazione/)*

MIGLIORANO LE STRATEGIE DI CYBERSECURITY, MA LE MINACCE CONTINUANO A EVOLVERE

21 aprile – E Mandiant ha presentato i risultati di *M-Trends 2023*, il report annuale sul panorama mondiale dei cyberattacchi basato sulle attività di investigazione e risposta dell'azienda. I risultati dell'indagine dimostrano **le organizzazioni sono riuscite a migliorare l'attività di cybersecurity, ma anche che gli attacchi sono in continua evoluzione e diventano sempre più sofisticati.** L'azienda ha osservato un **aumento del numero di incidenti segnalati da enti esterni rispetto a quelli interni.** Se si guarda al dettaglio delle singole aree, l'EMEA ha il più alto tasso di segnalazioni esterne (il 74%), mentre le Americhe registrano quello più basso (55%). Le due percentuali segnano però un importante aumento rispetto al 2021: l'EMEA contava un tasso del 60%, e le Americhe del 40%.

(source: https://www.uomoemanager.it/limportanza-dellaspetto-per-un-manager/)

L'IMPORTANZA DELL'ASPETTO PER UN MANAGER

20 aprile – Essere un buon manager non riguarda solo le abilità tecniche e la conoscenza del settore, ma anche l'aspetto esteriore.

L'abbigliamento e l'acconciatura possono avere un impatto significativo sull'immagine di un manager e sulla sua capacità di comunicare efficacemente con il suo team e i clienti.

(source: https://www.uomoemanager.it/limportanza-dellaspetto-per-un-manager/)

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

ISACA
Rome Chapter

CORSI ISACA

ATTIVITÀ FORMATIVA DI ISACA ROMA

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

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

ISACA
Rome Chapter

WHY SHOULD I CERTIFY WITH ISACA?

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

GET CERTIFIED

ISACA 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.