ISACA Rome Chapter

Newsletter

ANNO 2023 | N. 6 | GIUGNO

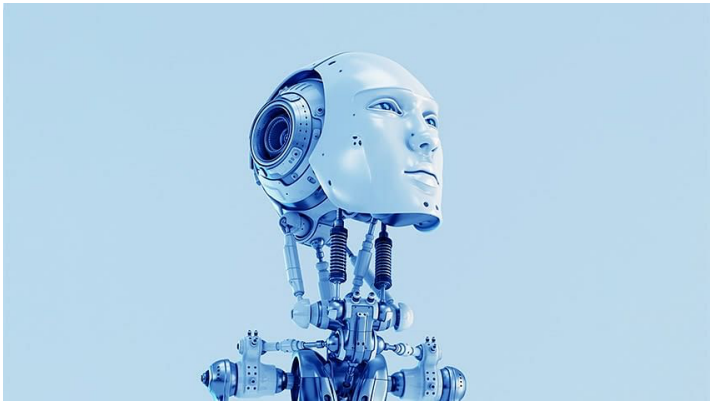
ISACA (Information Systems Audit and Control Association)

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

Safety, Cybersecurity delle AI: la standardizzazione come "chiave di volta"

Nella newsletter di febbraio abbiamo già iniziato a ragionare insieme di AI e delle implicazioni sulla sicurezza degli individui o dei rischi di un uso malevolo. La proposta di legge di *AI Act europeo* è stato un primo passo proprio in questa direzione e rappresenta di fatto la prima legge sull'intelligenza artificiale da parte di un organismo regolatore di rilievo. La legge assegna le applicazioni dell'AI a tre categorie di rischio: la prima è costituita dalle applicazioni e dai sistemi che creano un rischio inaccettabile: ne sono esempi la manipolazione cognitivo-comportamentale di persone o specifici gruppi vulnerabili quali giocattoli ad attivazione vocale che incoraggiano comportamenti pericolosi nei bambini; oppure il punteggio sociale di matrice cinese che classifica le persone in base al comportamento, allo stato socio-economico o alle caratteristiche personali; o anche i sistemi di identificazione biometrica remota e in tempo reale, come il riconoscimento facciale. Il secondo livello è costituito dalle applicazioni ad alto rischio che devono essere soggette a requisiti legali specifici. I sistemi di AI che incidono negativamente sulla sicurezza o sui diritti fondamentali considerati ad alto rischio sono suddivisi in due categorie: i Sistemi di intelligenza artificiale utilizzati nei prodotti che rientrano nella legislazione dell'UE sulla sicurezza dei prodotti (include giocattoli, aviazione, automobili, dispositivi medici e ascensori); i sistemi di AI che rientrano in otto aree specifiche che dovranno essere registrate in una banca dati dell'UE: identificazione biometrica e categorizzazione delle persone fisiche; gestione e funzionamento delle infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso e fruizione dei servizi privati essenziali e dei servizi e benefici pubblici; applicazione della legge; migrazione, asilo e gestione dei controlli alle frontiere; assistenza nell'interpretazione giuridica e nell'applicazione della legge.



Infine, ci sono le applicazioni non esplicitamente vietate perché non considerate ad alto rischio che quindi, in gran parte, sono lasciate non regolamentate.

Per i requisiti di trasparenza invece, l'AI generativa, (es. CHAT GPT), dovrebbe rispettare i requisiti di trasparenza: rivelare che il contenuto è stato generato dall'intelligenza artificiale, progettare il modello per evitare che generi contenuti illegali, pubblicare riepiloghi di dati protetti da copyright utilizzati per la formazione.

Per sostenere la decisione dei parlamentari europei sul testo in fase di proposta, l'ENISA (European Union Agency for Cybersecurity), Agenzia per la Sicurezza Europea, ha pubblicato nel marzo di quest'anno un documento dal titolo "*Cybersecurity of AI e Standardizzazione*", che fornisce una panoramica degli standard esistenti, in fase di elaborazione, in esame e pianificati, relativi alla sicurezza informatica

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

dell'intelligenza artificiale (AI), per valutarne la copertura e identificare le lacune nella standardizzazione. Per farlo il documento considera le specificità dell'AI come ad esempio l'apprendimento automatico, coniugando sia la visione della sicurezza informatica ricompresa nel paradigma "tradizionale" di riservatezza-integrità-disponibilità, sia il concetto più ampio di affidabilità dell'AI. Infine, la relazione esamina in che modo la normazione può sostenere l'attuazione degli aspetti di cybersicurezza (questi stessi criteri sono incorporati nella proposta di regolamento dell'UE dell' AI Act - COM 2021-206 final, n.d.r.).

Le conclusioni dello studio di ricerca e analisi hanno permesso di suggerire che gli standard generali per la sicurezza delle informazioni e la gestione della qualità (in particolare ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 9001) possono mitigare parzialmente i rischi di sicurezza informatica legati alla riservatezza, all'integrità e alla disponibilità dei sistemi di AI. Questa conclusione è basata sul presupposto che l'AI sia nella sua essenza software, e quindi ciò che è applicabile al software può essere applicato all'AI, se viene fornita una guida adeguata. Sebbene sia una generica raccomandazione, l'ENISA raccomanda un'integrazione basata su un'analisi specifica del sistema rispetto al dominio di applicazione (ad esempio basandosi su ISO/IEC 15408-1:2009).

Tuttavia, è ancora oggetto di dibattito fino a che punto la valutazione della conformità ai requisiti di sicurezza risultanti, possa basarsi su standard orizzontali specifici dell'AI e in che misura possa basarsi su standard verticali/settoriali specifici. Poiché la sicurezza informatica è trasversale a una serie di requisiti di affidabilità (ad esempio governance dei dati, trasparenza), è importante che le attività di standardizzazione relative a questi requisiti trattino la sicurezza informatica in modo coerente. Attualmente sono stati evidenziati dei gap di standardizzazione:

1. la tracciabilità dei dati e dei componenti dell'intelligenza artificiale durante il loro ciclo di vita resta un problema che attraversa la maggior parte delle minacce e rimane in gran parte irrisolto nella pratica;
2. le caratteristiche intrinseche del Machine learning non sono pienamente riflesse negli standard esistenti, soprattutto in termini di metriche e procedure di test;
3. in alcuni settori le tecnologie correlate sono ancora in fase di sviluppo e non sono ancora abbastanza mature per essere standardizzate (ovvero gli standard esistenti non possono essere adattati o i nuovi standard non possono ancora essere completamente definiti).

Per la messa in pratica della proposta di legge sull'AI act invece l'ENISA ha individuato che ad oggi non esistono norme che coprano adeguatamente la sicurezza informatica e descrivano le competenze delle organizzazioni per l'audit, la certificazione e il collaudo dei sistemi di AI (e dei sistemi di gestione dell'AI) e dei loro valutatori; tale lacuna nei settori oggetto di ricerca e sviluppo è rilevante per l'attuazione del progetto di legge sull'AI, in particolare per quanto riguarda le casistiche di dati alterati (*poisoning data*) e le applicazioni poste in essere dai criminali digitali.

Il testo dell'ENISA fornisce precise raccomandazioni finali su ogni fronte dei gap evidenziati e auspica un comune sforzo di continua analisi delle tecnologie in favore della standardizzazione come mezzo di supporto alla sicurezza informatica e un parallelo impegno per le valutazioni di conformità come guida della componente legislativa regolatoria.

Il 14 giugno 2023, i deputati hanno adottato una *posizione negoziale del Parlamento sulla legge* sull'AI che mira a garantire l'adozione di AI "sicure e trasparenti". Ora inizieranno i colloqui con i paesi dell'UE in sede di Consiglio sulla forma finale della legge. I materiali documentali e il documento fornito da ENISA costituiscono una solida base di lavoro.

L'obiettivo è raggiungere un accordo entro la fine di quest'anno.

Alessia Valentini
Cyber security consultant, CISA

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

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 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 la diffusione della digitalizzazione e dei servizi ad essa collegati i settori finanziario e fintech devono attrezzarsi e imparare a reagire tempestivamente alle minacce in continuo aumento di attacchi informatici.
Nel mese di dicembre scorso sono state pubblicate nella Gazzetta Ufficiale della UE:

- il Regolamento **DORA** (Digital Operational Resilience Act) per la difesa unica europea che ha l'obiettivo di disciplinare in maniera uniforme la "resilienza operativa" nel settore finanziario in tutta l'Europa;
- la Direttiva DORA;
- ed anche la NIS2.

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.

Rome - Italy ■ 5/7 October 2023

AEIT International 2023 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

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

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

LE PRINCIPALI NOTIZIE

INTELLIGENZA ARTIFICIALE: L'IMPATTO SUL FUTURO MONDO DEL LAVORO ED ECONOMICO FINO A 4,4 TRILIONI DI DOLLARI

02 luglio – L'Intelligenza Artificiale generativa è pronta a scatenare la prossima ondata di produttività. A indagarne portata e potenziale economico, stimato fino a 4,4 trilioni di dollari, è il recente studio intitolato "The economic potential of generative AI" e stilato da ***Mc Kinsey***, che la definisce la prossima frontiera della produttività. L'intelligenza artificiale ha permeato le nostre vite in modo incrementale. Le applicazioni come ChatGPT di ***OpenAI***, GitHub Copilot, Stable Diffusion e altre hanno catturato l'immaginazione delle persone in tutto il mondo in un modo che AlphaGo non ha fatto, grazie alla loro ampia utilità e all'abilità soprannaturale per avere una conversazione con un utente. La velocità con cui si sta sviluppando la tecnologia è sotto gli occhi di tutti.

(source: https://www.igizmo.it/intelligenza-artificiale-limpatto-sul-futuro-mondo-del-lavoro-ed-economico-fino-a-44-trilioni-di-dollari/)

COME SI INSINUA L'INTELLIGENZA ARTIFICIALE NELLE GRANDI BANCHE

02 luglio – Le grandi banche potrebbero non fidarsi di ChatGpt e, quindi, JP Morgan e Goldman Sachs stanno progettando i propri chatbot basati sull'intelligenza artificiale. Morgan Stanley, invece, ha stretto un accordo con OpenAI e una banca italiana ha stanziato 5 miliardi di euro per "tecnologia e crescita". Tutti i dettagli.

(source: https://www.startmag.it/innovazione/come-si-insinua-intelligenza-artificiale-nelle-grandi-banche/)

UE, VERSO NORME RAFFORZATE SULLA PRIVACY: LENTE SULLE BIG TECH

02 luglio – Aiutare le autorità nazionali per la **protezione dei dati a cooperare nelle indagini transfrontaliere**, comprese quelle sulle **Big Tech**.

È questo, in sintesi, il contenuto della proposta per rafforzare l'applicazione del regolamento Ue sulla privacy (Gdpr) che la Commissione europea si appresta a presentare **martedì 4 luglio**. Il piano, con l'introduzione di nuove regole procedurali comuni, "rafforzerà la fiducia dei cittadini facilitando una **risoluzione più rapida delle indagini** e riducendo il numero di dispute tra le autorità di controllo" dei Ventisette "nei casi transfrontalieri", si legge nell'ultima bozza della proposta.

Il Gdpr, **regolamento generale sulla protezione dei dati,** ufficialmente **regolamento (UE) n. 2016/679**, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016.

(source: https://www.rainews.it/articoli/2023/07/ue-verso-norme-rafforzate-sulla-privacy-lente-su-big-tech-c351fead-0afe-40f3-b855-47b7ea8b9eb1.html)

IL GOVERNO HA ADOTTATO LA PRIMA STRATEGIA DI SICUREZZA NAZIONALE NELLA STORIA DELLA GERMANIA

26 giugno – **Per la prima volta la Germania ha una strategia di sicurezza nazionale. Ma non è chiaro come il governo potrà attuare il nuovo piano militare e di politica estera**

Dopo mesi di negoziati, mercoledì 14 giugno il cancelliere tedesco Olaf Scholz e i più importanti ministri hanno presentato **la prima Strategia di sicurezza nazionale**. Il gabinetto ha approvato il documento di 76 pagine in cui descrive i propri **obiettivi futuri riguardo le relazioni internazionali della Germania**, nel contesto del conflitto in Ucraina e della crescita della potenza cinese.

(source: https://berlinomagazine.com/2023-il-governo-ha-adottato-la-prima-strategia-di-sicurezza-nazionale-nella-storia-della-germania/?expand_article=1)

ePROCUREMENT PER GLI APPALTI, ECCO LE REGOLE TECNICHE AGID PER LE PIATTAFORME

21 giugno – Agid ha approvato un provvedimento con cui sono state dettate le regole tecniche sulle piattaforme di approvvigionamento digitale. Definiti caratteristiche e meccanismi di certificazione e introdotte specifiche previsioni volte a "governare" quei sistemi che opereranno attraverso tecnologie basate su registri distribuiti. Il "Nuovo Codice dei contratti pubblici" (il D.lgs. n. 36/2023), pubblicato in Gazzetta Ufficiale lo scorso 31 marzo e che diventerà efficace a partire dal prossimo primo luglio 2023, vede nella digitalizzazione del processo di approvvigionamento uno dei propri punti di forza.

(source: https://www.agendadigitale.eu/procurement/eprocurement-per-gli-appalti-ecco-le-regole-tecniche-agid-per-le-piattaforme/)

CYBER SECURITY E SICUREZZA DELLE INFORMAZIONI: QUANDO IL FATTORE UMANO E LA TECNOLOGIA HANNO LA STESSA IMPORTANZA

23 giugno – I moderni servizi di conservazione a lungo termine in cloud costituiscono oggi un'opzione importante per la sicurezza delle informazioni rispetto a errori umani e agli attacchi di cyber security. Vediamo quali sono le caratteristiche e prerogative più utili. Nell'affrontare ***le tematiche di cyber security e di sicurezza dei dati*** si fa spesso l'errore di concentrarsi solo sulle **infrastrutture digitali** dimenticandosi di considerare il **fattore umano**. Un buon livello di sicurezza richiede tecnologie aggiornate, ma anche una gestione senza imprevisti e utenti che non si facciano abbindolare dalle e-mail di ***phishing*** o dalle richieste di password via e-mail inviate dall'indirizzo contraffatto di un collega.

(source: https://www.cybersecurity360.it/legal/privacy-dati-personali/cybersecurity-sicurezza-informazioni-fattore-umano-tecnologia/)

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

RELAZIONE ANNUALE ACN, COME L'ITALIA AFFRONTA IL PICCO DEL CYBERCRIME

23 giugno – È di recente pubblicazione la nuova Relazione Annuale dell'ACN sulle attività, i dati e i progetti riferiti al 2022 in materia di cybersicurezza. Un anno intenso, ma anche di crescita, per l'Agenzia per la cybersicurezza nazionale. **Cresce** l'attività **malevola** in campo cyber ai danni di enti governativi, infrastrutture critiche e operatori privati in Italia.
Lo rivelano i dati della Relazione annuale riferita all'anno 2022 dell'***ACN*, l'Agenzia per la cybersicurezza nazionale**, che raccoglie tutti i dati e i progetti dell'Agenzia e che testimonia l'intensità delle sue **attività e le sfide** che ha dovuto affrontare seguendo le direttive della Strategia Nazionale di Cybersicurezza 2022-2026 per il potenziamento della sicurezza del nostro Paese.
(source: https://www.agendadigitale.eu/sicurezza/relazione-annuale-acn-come-litalia-affronta-il-picco-del-cybercrime/)

CYBERSECURITY: CHE COS'ABBIAMO IMPARATO IN 20 ANNI

26 giugno – Il progresso del cybercrime nella produzione di malware è impressionante. Ne danno una chiara idea i calcoli di Barracuda Networks: attualmente **i malware conosciuti sono più di un miliardo**, nel 2009 erano solo 25 milioni. E di quelli odierni, 94 milioni sono comparsi solo negli ultimi 12 mesi. Il vendor di soluzioni per la sicurezza informatica ha approfittato del ventesimo anniversario di attività per tracciare la linea evolutiva del malware dal 2003 ad oggi e ci sono alcuni elementi che danno da pensare.

(source: https://www.securityopenlab.it/news/2724/cybersecurity-che-cosabbiamo-imparato-in-20-anni.html)

CYBERSECURITY: UN ATTACCO OGNI TRE GIORNI

28 giugno – ***Si intensificano gli attacchi cyber ai danni di settori governativi e infrastrutture critiche, in particolare dell'ambito sanitario ed energetico. È quanto emerge dalla relazione annuale relativa al 2022, presentata il 19 giugno in Parlamento dall'Agenzia per la cybersicurezza italiana.***
Nel 2022 sono stati **1094 gli eventi cyber trattati** dal CSIRT (il team tecnico-operativo di prevenzione e risposta agli eventi informatici dell'ACN). In particolare, 130 sono gli **attacchi ai danni di uffici pubblici e aziende**, uno ogni tre giorni, in grado talvolta di bloccare i sistemi e **procurare ritardi nell'erogazione dei servizi**. Solo nel mese di febbraio, inoltre, sono stati analizzati 118 casi, in concomitanza allo **scoppio del conflitto in Ucraina**, benzina sul fuoco delle attività di hackeraggio.
(source: https://www.semprenews.it/news/Impennano-gli-attacchi-cyber-al-via-progetti-e-misure-per-rafforzare-la-sicurezza-nazionale.html)

BAIDU DICE CHE LA SUA INTELLIGENZA ARTIFICIALE È MIGLIORE DI CHATGPT

27 giugno – **Baidu**, la compagnia proprietaria del motore di ricerca leader in Cina, *ha affermato* che l'ultima versione del suo chatbot AI **ha superato il popolare competitor** ChatGpt su alcune metriche chiave. Più nel dettaglio, come riportato dal *China Science Daily*, **Ernie 3.5** ha superato ChatGpt "*nei punteggi di abilità completi*" e ha **battuto Gpt-4**, l'ultimo e più avanzato modello di OpenAI, **nei test di lingua cinese**. Tuttavia, l'AI di Baidu si è posizionata dietro a *Gpt-4* per i test di lingua inglese, seppur comunque davanti a ChatGpt. Ma questo non è stato il solo test a cui è stato sottoposto il chatbot della compagnia cinese.
In un test in lingua cinese contenente **oltre 13.000 domande** a scelta multipla **su più di 50 argomenti diversi**, Ernie 3.5 si è dimostrato essere migliore dei due modelli competitor di OpenAI. Infine, in un test sviluppato da un gruppo di università statunitensi su temi come scienze e discipline umanistiche, il chatbot di Baidu si è dimostrato ben peggiore di ChatGpt e Gpt-4. Insomma, nel complesso Ernie 3.5 ha mostrato di aver ottenuto importanti miglioramenti in poco tempo.
(source: https://www.wired.it/article/baidu-intelligenza-artificiale-chatgpt/)

A CHI APPARTIENE UN'OPERA CREATA DALL'INTELLIGENZA ARTIFICIALE?

28 giugno – Come conciliare l'avvento dell'*intelligenza artificiale* con la creatività e quali nuove frontiere dell'insegnamento si manifestano con l'***arte* generativa**? Se ne è discusso a Roma durante l'evento Ai Bounds organizzato nell'aula magna dell'Accademia delle arti e nuove tecnologie (Aant). Le **più importanti accademie della capitale** si sono confrontate su quali dovranno essere le nuove competenze che gli studenti dovranno acquisire nell'uso dell'Ai per creare opere mantenendo uno "*spirito critico ed etico*". All'incontro, patrocinato dall'Associazione per il disegno industriale del *Lazio* (Adi) hanno preso parte Rossana Quarta di Aant, Laura Negrini dello **Ied di Roma**, Silvia Simoncelli della **Naba di Roma**, Fabio Mongelli della **Rufa**. Ad aprire i lavori il sociologo Derrick De Kerckhove e quella del legale Luca Amorelli.
(source: https://www.wired.it/article/intelligenza-artificiale-generativa-arte-futuro-diritto-autore/)

CYBERSECURITY: DIFENDI E PROTEGGI LA TUA AZIENDA

29 giugno – **Gli attacchi informatici aumentano costantemente**: il 67% delle aziende in Italia ha rilevato una crescita del numero dei tentativi di cyber attacco durante il corso dello scorso anno, con il 14% che ha subito delle conseguenze tangibili, come interruzioni del servizio, ritardi nello svolgimento delle operazioni o addirittura danni reputazionali.
Ecco perché l'attenzione verso il tema della **cybersecurity** è sempre più accesa in Italia, tanto da confermarsi **nel 2023** come la **principale priorità di investimento** per il 61% delle imprese e organizzazioni al di sopra dei 250 addetti. Secondo i risultati della ricerca dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, complessivamente nel 2022 il mercato italiano della cybersecurity ha raggiunto il valore di 1,86 miliardi di euro, con un aumento del +18% rispetto al 2021.
(source: https://www.engage.it/tecnologia/cybersecurity-difendi-e-proteggi-la-tua-azienda.aspx)

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

ISACA Rome Chapter

Newsletter

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

Social Media

http://www.isacaroma.it/

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.

GET CERTIFIED

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

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.