ISACA Rome Chapter

Newsletter

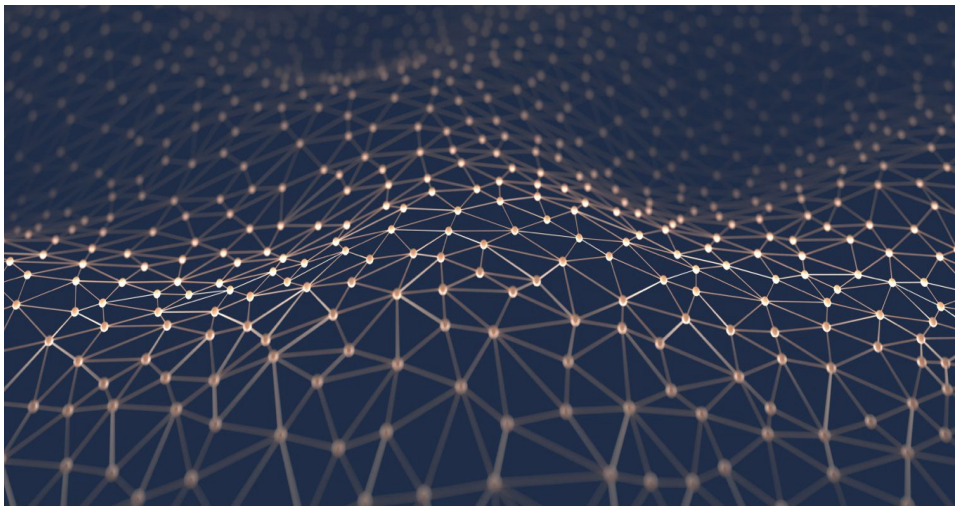
ANNO 2023 | N. 8 | SETTEMBRE

ISACA (Information Systems Audit and Control Association)

L'*ISACA*, (Information Systems Audit and Control Association), ha 158.998 associati in oltre 188 nazioni (dato aggiornato al 30 giugno 2023) ed è 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'USO DELLE GAN (GENERATIVE ADVERSARIAL NETWORK) PER LA CYBERSECURITY



L'Intelligenza Artificiale di tipo generativo utilizzata per la sicurezza informatica comporta l'applicazione di modelli specifici finalizzati a migliorare le misure di sicurezza, rilevare minacce informatiche e creare robusti meccanismi di difesa. Questi modelli generativi sono caratterizzati da un apprendimento delle strutture dei dati campione, che permette loro di generare nuovi campioni di dati sintetici in tutto e per tutto somiglianti ai dati originali. Nel contesto della sicurezza informatica, tale peculiarità si rivela utile per il rilevamento di anomalie (anomaly detection), l'arricchimento dei dati (data augmentation) e la simulazione di attacchi avversari (Adversarial Attack Simulation). Esempi di tali modelli generativi sono le Variational Autoencoder (VAE), i modelli basati su Transformer e le *Generative Adversarial Networks (GAN)*.

Le GAN sono una classe di modelli generativi costituiti da due reti neurali, un generatore e un discriminatore, addestrate simultaneamente in un gioco a somma zero. Il generatore crea campioni di dati sintetici, mentre il discriminatore valuta l'autenticità sia dei campioni reali sia di quelli generati. L'obiettivo del generatore è creare campioni indistinguibili dai dati reali, mentre l'obiettivo del discriminatore è classificare accuratamente i campioni come reali o generati. Questo modello si chiama sistema di Machine Learning supervisionato perché avviene una correzione del modello mediante sistemi di regressione logica (Fonte *Jason Brawnlee*).

Il creatore delle GAN è *Ian J. Goodfellow* che fin dal 2014 aveva studiato presso la University of Montreal e pubblicato il primo *paper scientifico sulle Generative adversarial Networks (GAN)*. Yann LeCun, professore alla New York University, VP & Chief AI Scientist at Meta e pioniere insieme a Geoffrey Hinton, della rivoluzione moderna nelle reti neurali profonde, le considera "la più interessante idea nell'ambito del Machine Learning negli ultimi 10 anni" (Fonte *IEEE.Org*).

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

Per approfondire questi modelli e capirne la struttura logica e il funzionamento è possibile consultare la pagina *Developers di Google dedicata alle GAN*

Proprio le GAN nella Cybersecurity sono utili per generare modelli di traffico di rete realistici, simulare attacchi informatici e creare set di dati sintetici per l'addestramento di modelli di machine learning. Se ad esempio si prendono degli esempi di malware e di applicazioni benigne, sapendo distinguere la natura per ognuno di questi esempi, allora, applicandolo ad una GAN il sistema di Machine Learning sarà in grado di addestrare un classificatore per etichettare esempi futuri, riuscendo a distinguere il malware dalle applicazioni vere e proprie. Questo perché inizialmente il generatore non sa nulla e genera esempi iniziando da dati random mentre il classificatore che usa Machine Learning su dati reali, inizia a distinguere i dati "fake" generati da quelli reali. Quando la decisione del classificatore torna come feedback al generatore, quest'ultimo comincia ad apprendere tanto da generare dati più credibili. Il ciclo reiterato progressivamente migliora il set di dati generati, tanto che dopo un sufficiente numero di interazioni, i dati generati sono fattivamente indistinguibili da quelli veri.

Un ulteriore utilizzo delle GAN riguarda le applicazioni di image processing tanto da essere in grado di generare immagini artificiali perfettamente realistiche. Il rischio correlato a questa capacità è legato al fenomeno dei deep fake e di un uso malevolo di tali immagini non reali, che sembrano vere per costruire fenomeni di fake news. In questi casi, spiega il prof. Bergadano Ph.D. e professore ordinario di informatica, sicurezza informatica e identity management presso l'Università di Torino, "*i sistemi di riconoscimento utente basati ad esempio su impronta digitale, keystroke dynamics o riconoscimento della voce non possono prescindere dall'utilizzo di tecniche adversarial, e devono impedire l'utilizzo del classificatore come black box, perché potrebbe essere utilizzato in modo malevolo per allenare il generatore di una GAN*".

In effetti nell'ambito della Cybersecurity si può verificare un utilizzo distorto: potendo generare dati falsi, che però sembrano veri, si può facilmente ottenere la cosiddetta "evasion" di un sistema di sicurezza, evitando la generazione di allarmi e riuscendo a battere i sistemi di autenticazione biometrica. Questo significa che i sistemi GAN usati dagli avversari digitali permettono di aggirare allarmi e strumenti di controllo di accesso che sono stati appresi in base ai dati disponibili.

D'altra parte, le GAN usate con lo stesso criterio per la difesa, sono applicabili nella anomaly detection e per irrobustire i sistemi di autenticazione affinché siano maggiormente capaci di resistere agli attacchi informatici. Lo stesso tipo di dinamica si verifica per l'individuazione delle intrusioni in rete solitamente protetta da sistemi IDS (Intrusion Detection systems): i criminali possono aggirare un IDS mediante un sistema GAN dotato di un classificatore simile all'IDS e di un generatore che a un certo punto del suo addestramento potrà essere in grado di attuare intrusioni non rilevabili. Ma anche qui, per difendersi da questa situazione sono stati realizzati sistemi di intrusion detection "adversarial", basati su chiavi segrete. Anche nei casi di web e application defacement le tecniche di evasione basate su "adversarial networks" possono essere fermate mediante l'utilizzo di randomizzazione e chiavi segrete. In sostanza per una difesa efficace mediante GAN è necessario introdurre la randomizzazione e/o informazioni segrete nella fase di Machine Learning (che diventa così una black box per gli avversari) in modo da evitare l'uso malevolo dei classificatori. Infine, il prof. Bergadano ha spiegato (Fonte *Proactive password checking*) che nel contesto dei controlli delle password l'utilizzo delle GAN è consigliato se associato ad un dizionario di password: "la password deve essere rifiutata se è "simile" a parole presenti in un dato dizionario. Questo perché, attraverso una GAN, è possibile generare un gran numero di password a partire da un dizionario, come dimostrato dal *sistema PassGAN* che allenandosi sul dizionario "rockyou", ha dimostrato di poter riconoscere il 24,2% del password leak di Linkedin, che a sua volta, non aveva relazione con il dataset di partenza".

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.

ISACA Rome Chapter

Newsletter

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

LA STARTUP ITALIANA CHE CREA DATI SINTETICI PER ADDESTRARE L'INTELLIGENZA ARTIFICIALE

24 settembre – L'***intelligenza artificiale*** **generativa** ha bisogno di nutrirsi di molti, **moltissimi dati** per addestrare i propri algoritmi ed essere davvero utile alle aziende e alle organizzazioni. Questi **dataset** si stanno rivelando il cuore del nascente *business* dell'AI, in qualche modo a valle degli stessi modelli generativi, perché quasi nessuno dispone di corpus "puliti", affidabili, completi e inclusivi. La nostra è la fase dei cosiddetti **dataset "sporchi" o scadenti**: pieni di buchi, errori, pregiudizi, informazioni certi massicce ma spesso parziali, che non "coprono" in modo uniforme e completo un certo ambito, fenomeno, settore o categoria. E alla fine rischiano di creare più danni che benefici a chi li impiega come base di partenza per allenare i propri strumenti di intelligenza artificiale. Una *startup* italiana, ***Clearbox AI***, ha la soluzione: i dati sintetici.

(source: https://www.wired.it/article/intelligenza-artificiale-clearbox-ai-dati-sintetici-privacy/)

P.A. AUMENTA LA SPESA PER LA CYBERSICUREZZA

24 settembre – Secondo il ***Threat Intelligence Report 2022*** elaborato dall'Osservatorio Cybersecurity di Exprivia, la cyber-sicurezza è diventata fondamentale anche per la Pubblica Amministrazione.
Dal Report emerge che nel 2022 tra pubblico e privato si sono verificati circa 2.600 casi di cyber-crime, quasi il doppio rispetto ai 1.356 del 2021 e più del quadruplo rispetto ai 605 del 2020. Di questi 2.600 casi, 260 hanno interessato la Pubblica Amministrazione.
Si tratta di dati abbastanza diversi da quelli raccolti nella Relazione annuale dall'Agenzia per la Cybersicurezza Nazionale (ACN), dove, nel 2022, i casi totali sono stati 1.094, di cui il 18% a danno della P.A. Probabilmente la differenza dipende dai criteri di rilevazioni adottati.

(source: https://www.uilpa.it/p-a-aumenta-la-spesa-per-la-cybersicurezza/)

L'INTERVISTA: PRIVACY E CYBERSECURITY. UNA SFIDA CHE COMINCIA DALLE POSTAZIONI DI LAVORO. SE NE PARLA IL 4/10 A LUGANO IN UN EVENTO

25 settembre – Non c'è bisogno di andare troppo in là con l'immaginazione, per avere a che fare con la **cybersecurity**. Nessuna stanza segreta, niente nomi altisonanti o rivalità politiche che sfociano in una guerra attraverso i meandri del web; a volte, anzi molto più spesso, la sfida è **nelle cose piccole**. Come un telefonino utilizzato per connettersi alla rete fuori ufficio, una postazione di lavoro sulla carta ben organizzata. Comincia da qui, dal quotidiano e dagli spazi apparentemente sicuri di un'azienda, la **protezione dei dati**, da mettere al riparo dalle intenzioni più cattive: un tema sempre caldo e attuale che, declinato in questa accezione, sarà oggetto di un evento dedicato **il 4 ottobre all'Hotel Dante di Lugano**.

(source: https://www.moneymag.ch/privacy-cybersecutity-evento)

COSA VUOLE FARE IL GOVERNO SULL'INTELLIGENZA ARTIFICIALE

23 settembre – L'intelligenza artificiale è un mondo che sta entrando prepotentemente nella nostra realtà di tutti i giorni, che non possiamo in alcun modo ignorare, ma che al contrario dobbiamo saper conoscere, gestire e regolare.
Viviamo in uno scenario complesso, visto che da sempre la tecnologia ha influito sul nostro modo di vivere, ma oggi la diversità è rappresentata dalla "velocità" del cambiamento e da un cambiamento che incide non più solo sulle cose, ma sulla nostra "cognitività".

(source: https://www.startmag.it/innovazione/governo-intelligenza-artificiale/)

L'AZIENDA INFORMATICA CISCO ACQUISIRÀ LA SOCIETÀ DI SOFTWARE PER LA CYBERSICUREZZA SPLUNK PER 28 MILIARDI DI DOLLARI

21 settembre – L'azienda informatica Cisco acquisirà la società produttrice di software Splunk per 28 miliardi di dollari (circa 26 miliardi di euro). Cisco è specializzata nella produzione di hardware (cioè prodotti fisici) per le reti, mentre Splunk è specializzata nella produzione di programmi per la cybersicurezza. Per Cisco, già fra le più importanti società informatiche al mondo, è l'acquisizione più grande di sempre, e la renderà una delle più grandi aziende di software. Secondo ***Bloomberg***, Cisco sta cercando di dipendere sempre meno dal suo business originale, cioè la vendita di apparecchiature per il funzionamento delle reti di computer.

(source: https://www.ilpost.it/2023/09/21/cisco-acquisizione-splunk/)

UNA GUIDA PER INSERIRE L'INTELLIGENZA ARTIFICIALE IN AZIENDA IN MODO RESPONSABILE

22 settembre – Un bel mattino ci siamo accorti che la tecnologia ha fatto passi da gigante, costringendoci a una rincorsa affannosa, perfino sul piano etico. **L'*intelligenza artificiale* (AI)** sta rapidamente **rivoluzionando il modo in cui le imprese operano e interagiscono con il mondo**. Con il suo crescente impatto in settori come la produzione, il marketing e la logistica, è diventato fondamentale per le aziende **comprendere come utilizzare l'AI in modo responsabile**, per non rimanere indietro. In risposta a questa esigenza, **il Cefriel**, centro di innovazione digitale affiliato al Politecnico di Milano, **ha pubblicato lo studio *Intelligenza artificiale responsabile***, in cui Diego Ragazzi,

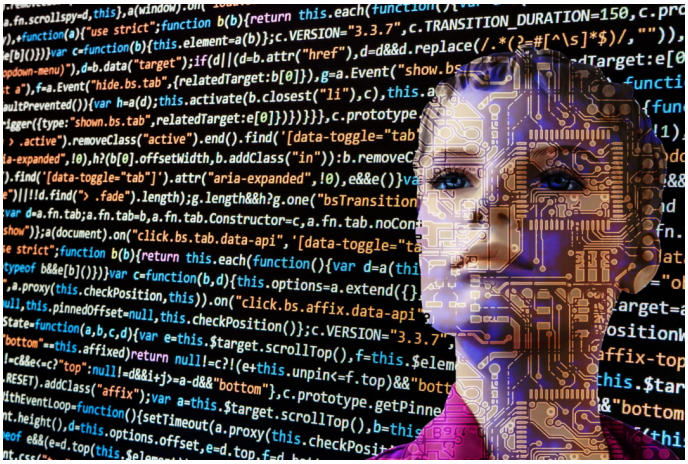
ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

esperto senior di Data strategy al Cefriel, riflette su rischi e responsabilità che questa tecnologia genera.
(source: https://www.wired.it/article/intelligenza-artificiale-etica-imprese-guida-strategica/)

I CYBER-AGENTI SONO LIBERI DI HACKERARE

22 settembre – *I cyber-agenti infiltrati devono aver* ***libertà di hackerare***. Non devono essere punibili se, al fine di contrastare eversione e terrorismo, decidono di aprire **account** e **siti fake**, accedendo o alterando i sistemi telematici e informatici.
Questo è quanto proposto da un emendamento che vede la firma dei relatori **Pietro Pittalis** e **Sara Kelany** al disegno di legge in conversione del **DL 105/2023**, in esame in commissione alla Camera. L'emendamento, in sintesi, rafforza gli strumenti atti al contrasto di eversori e terroristi, che pianificano e realizzano, sempre più spesso, attività delittuose, utilizzando il web.
Nella strategia che è stata disegnata nell'emendamento sono previste tre linee di intervento. La prima riguarda i margini di manovra per le **operazioni sotto copertura**, per combattere l'eversione e il terrorismo, ma anche i reati informatici che interessano le varie infrastrutture critiche informatizzate.
(source: https://servicematica.com/i-cyber-agenti-sono-liberi-di-hackerare/)

DELL'INTELLIGENZA ARTIFICIALE. E NONDIMENO UMANA.



21 settembre – In occasione della recente inaugurazione dell'anno accademico dell'Università della Calabria, alla presenza del ministro dell'università Anna Maria Bernini, Georg Gottlob, noto scienziato dell'IA, l'Intelligenza Artificiale, ha tenuto una *lectio magistralis* su "Intelligenza e ignoranza artificiale". Una replica, pacata e argomentata, e non proprio implicita, a quanti manifestano crescenti sintomi di apprensione, se non di angoscia, nella convinzione che le nuove generazioni, definite "digitali", saranno le prime della Storia in cui i figli sono destinati a scontare un profondo degrado nel rapporto con la costellazione dei saperi, rispetto ai loro genitori, "a causa della tecnologia".
(source: https://www.micromega.net/l-intelligenza-artificiale-resta-solo-unimitazione-di-quella-umana/)

SUPER COMPUTER E AI: STRUMENTI CONTRO IL CYBERCRIME

21 settembre – L'Intelligenza artificiale rappresenta un asset strategico rivoluzionario, che può essere impiegato anche per **contrastare i cyber attack**. Il tessuto industriale italiano, e, dal canto suo la pubblica amministrazione, rappresentano una 'superficie digitale' da proteggere dagli attacchi informatici. E questo è possibile grazie a un uso responsabile dei sistemi di intelligenza artificiale.
Su questa tesi si è basato l'intervento di **Bruno Frattasi**, **direttore generale dell'Agenzia per la cybersicurezza nazionale (Acn)**, nell'ambito del convegno ***"Intelligenza artificiale: creatività, etica, diritto e mercato"***. Abbiamo voluto approfondire il tema, intervistando **Frattasi** su alcuni aspetti che vedono coinvolta attivamente l'Acn.
(source: https://www.fortuneita.com/2023/09/21/super-computer-e-ai-strumenti-contro-il-cybercrime/)

NASCE HWG SABABA DALL'ESPERIENZA DI DUE GRANDI REALTÀ ITALIANE DELLA CYBERSECURITY

21 settembre – Nasce HWG SABABA, con l'accordo tra HWG, azienda specializzata nell'erogazione di servizi gestiti e consulenza in ambito cyber e Sababa Security, primario fornitore di cybersecurity di soluzioni di sicurezza integrate per la protezione dell'IT, OT e ambienti IoT. Una nuova, unica, azienda italiana capace di affrontare le crescenti sfide legate al mercato della cyber sicurezza nazionale ed internazionale. In un settore in continua evoluzione, dove le minacce informatiche si evolvono rapidamente, sfruttando gli estesi perimetri digitali che le aziende hanno ampliato oltre la propria infrastruttura IT, è essenziale rispondere con tecnologie all'avanguardia, i migliori talenti, la continua innovazione e l'anticipazione delle dinamiche dello scenario, condividendo le migliori strategie di protezione con le istituzioni nazionali di riferimento per salvaguardare i dati sensibili in tutti i settori, dagli asset più rilevanti del Paese, alle singole aziende private. HWG Sababa nasce con questo obiettivo: consolidare la posizione di riferimento in Italia e nell'area mediterranea di due grandi player della cybersecurity che unendosi sono oggi in grado di far fronte a tutte le necessità di protezione con servizi specializzati e completi.
(source: https://www.romadailynews.it/attualita/nasce-hwg-sababa-dall-esperienza-di-due-grandi-realta-italiane-della-cybersecurity-0740996/)

WHAT IS A DATA BREACH? DEFINITION, EXAMPLES & PREVENTION

20 settembre – A data breach occurs when unauthorized individuals gain access to confidential information. The consequences of a data breach can be severe and far-reaching. Hackers can use compromised data for illegal activities including identity theft, financial fraud, spamming or even extortion. In this article, we'll do a deep dive into this topic so your organization will be more proactive in preventing this risky incident.
(source: https://www.forbes.com/advisor/business/what-is-data-breach/)

GESTIONE DEI COOKIE DEL SITO WEB AZIENDALE: GUIDA PRATICA IN CHIAVE GDPR

20 settembre – Il sito web sembra ormai rappresentare una vera e propria necessità per qualsiasi azienda, in ottica reputazionale e di business. La corretta impostazione di un sito, tuttavia, passa anche dal rispetto di specifici obblighi normativi in materia di protezione dei dati personali
(source: https://www.agendadigitale.eu/sicurezza/privacy/gestione-dei-cookie-del-sito-web-aziendale-guida-pratica-in-chiave-gdpr/)

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

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

Master di I Livello in Sicurezza dei Sistemi e delle Reti

Master di I Livello in Cybercrime ed Informatica forense

Master di II Livello in Governance e Audit dei Sistemi Informativi

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.

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.