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

Newsletter

ANNO 2020 N. 07 LUGLIO-AGOSTO 2020

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha più di 145.000 associati in oltre 188 nazioni (dato aggiornato al 2019) 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) e CRISC (Certified in Risk and Information Systems Control). 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

La convergenza tra ICT e OT, un percorso lungo e complesso

Risale al 2002 il mio primo seminario di Sicurezza Informatica alla Scuola di perfezionamento in Prevenzione e Sicurezza della facoltà di Ingegneria a Roma. Per diversi anni ho continuato ad insegnare alla Scuola che nel frattempo si era trasformata in Master di II livello Cosa comunicavo allora e cosa ho imparato dagli ingegneri che si occupavano di prevenzione e sicurezza (safety e security) in impianti industriali di tutti i tipi? Quanto è cambiata la situazione in tutti questi anni? Mi sembra sempre valida la constatazione che i minori costi del mondo ICT, dovuti alla diffusione di massa delle relative tecnologie, e la loro enorme adattabilità per la risoluzione dei problemi più disparati erano allora, e sono tuttora, il motore economico inarrestabile per l'utilizzo delle tecnologie ICT in ogni campo possibile, incluso l'ambito OT (Operational Technology), ossia quei sistemi (PLC, SCADA, DCS, ecc.) che governano i processi industriali (Industrial Control Systems). Quindi era importante che ci si preparasse a tale evoluzione che avrebbe comportato l'esposizione del mondo OT al flusso continuo di minacce e vulnerabilità che le tecnologie ICT comportano.

D'altra parte, i processi industriali hanno complessità e vincoli che vanno compresi e impongono un approccio diverso. Il mondo OT è vincolato da leggi e regolamenti che hanno come obiettivo la tutela della safety e dell'ambiente perché un malfunzionamento può provocare feriti, morti, inquinamento, fermi di impianti critici per l'attività di una o più nazioni, ecc. Nel mondo ICT il malfunzionamento di un programma può provocare perdita di dati, furto di denaro, sanzioni pecuniarie e anche condanne penali ma normalmente nessuno si fa male fisicamente e nessuna città deve essere evacuata per un tempo anche lungo.

Ogni cambiamento in ambito industriale comporta quasi sempre analisi dei rischi, verifiche, eventuali nuove certificazioni, pianificazione, in sintesi una serie di processi che richiedono tempo e risorse. Nel mondo ICT se un software non funziona bene o deve essere migliorato, se ne distribuisce una nuova versione e la concorrenza tra aziende si basa anche sulla velocità di produrre software sempre nuovo e rapidamente disponibile, poi se ci sono dei bug si farà un nuovo release.

Siamo in presenza di ambiti che hanno velocità di evoluzione e vincoli molto diversi, potremmo dire che le tecnologie ICT viaggiano in aereo mentre il mondo OT si muove al massimo in nave, di converso i processi industriali hanno regole che li fanno somigliare a una società bene organizzata rispetto al Far West che spesso sembra regnare nella tecnologia delle informazioni.

Negli ultimi anni l'attenzione della ricerca scientifica, degli enti di standardizzazione e delle principali aziende ICT si è focalizzata sulla convergenza ICT e OT anche alla luce delle possibili applicazioni di nuove tecnologie ai processi industriali, tutto ciò anche grazie a piani di sviluppo sostenuti da programmi governativi e comunitari come nella UE.

Concetti come IoT (Internet of Things), IIoT (Industrial Internet of Things), Big Data sono divenuti una realtà diffusa e utilizzata. In particolare, la diffusione di IIoT, ossia di apparati industriali delle tipologie più varie connessi in rete, sta progressivamente dissolvendo il concetto di perimetro di impianto industriale e anche quello di perimetro di sicurezza, così come sta accadendo, o forse è già accaduto, nel mondo ICT. È opportuno evidenziare che nel prossimo futuro il concetto di IIoT verrà probabilmente assorbito da quello più generale di IoT, di cui gli apparati industriali costituiranno una particolare categoria, caratterizzata da standard e normative di safety e security che li renderanno idonei all'uso nei processi produttivi.

Le posizioni di enti come ENISA[1], NIST[2], ISO[3], ISA[4], IEEE[5], per citare quelli maggiormente rilevanti nei due ambiti, si suddividono in due approcci diversi e complementari. Il primo, rappresentato da ENISA vede gli IoT industriali come ecosistema che include gli apparati sul campo, le reti di connessione e i processi di elaborazione e controllo dei dati; quindi una convergenza tra l'ambito OT e ICT. Il secondo approccio, declinato dagli altri enti, ha il focus sulle caratteristiche degli apparati, inclusi i requisiti di sicurezza, e sull'interfaccia con i sistemi di livello superiore e la rete.

Sono i due classici approcci top-down e bottom-up, ma il vero problema è rappresentato dall'enorme varietà di apparati esistenti e le priorità da attribuire alla standardizzazione di un settore industriale piuttosto che ad un altro. Allo stato il lavoro di standardizzazione degli apparati è molto intenso negli enti come ISO e ISA, tradizionalmente attivi nel campo, ma la sensazione è che l'avvento degli IoT si sia concretizzato con una velocità superiore a quella con cui i tradizionali standard bodies sono in grado di reagire.

La visione top-down adottata da ENISA ha il vantaggio di affrontare il problema nel suo complesso anche se poi l'ecosistema IoT ipotizzato deve essere contestualizzato ad uno specifico settore come le infrastrutture critiche di comunicazione o lo Smart Manufacturing che sono quelli sinora esaminati dall'agenzia europea.

Negli ultimissimi anni la possibile convergenza sta subendo una notevole accelerazione, ci sono continue e numerose offerte di webinar, corsi, white paper, ecc. sulla sicurezza degli apparati industriali da parte di aziende del mondo ICT. Analogamente sono numerose le offerte di aziende specializzate in ambito industriale che offrono consulenze per gli aspetti, specie di sicurezza, relativi all'uso delle nuove tecnologie. Infine, alcuni giorni fa Microsoft ha acquisito un'azienda israeliana specializzata in ambito IIoT.

Per rappresentare lo stato attuale della convergenza forse è opportuno citare un breve webinar ISA nel quale un ex specialista dell'US Air Force raccomandava la formazione di team misti di personale ICT e OT per superare, dopo un training iniziale di tipo tecnico, la differenza culturale e la conseguente diffidenza tra persone che svolgevano essenzialmente lo stesso lavoro con due approcci diversi.

A mio parere quando gli ostacoli sono rappresentati da una "differenza culturale" la convergenza tecnica è già risolta o è in avanzata fase di risoluzione, rimane quella tra le persone o meglio la capacità di avere una visione più ampia che includa anche la visione dell'altro settore. È un percorso che richiederà del tempo ma l'evoluzione tecnica probabilmente lo accelererà.

---

[1] ENISA (European Union Agency for Network And Information Security)
[2] NIST (National Institute of Standards and Technology)
[3] ISO (International Standard Organization)
[4] ISA (International Society of Automation)
[5] IEEE (Institute of Electrical and Electronics Engineers)

Per completare il quadro è opportuno citare che oramai si parla di Industry 5.0, forse per indicare l'impatto che alcune nuove tecnologie come il 5G, un uso più intensivo dell'AI e concetti come l'Edge computing avranno sul mondo, industriale e non, nei prossimi anni. Ma forse allora non parleremo più di convergenza ICT/OT.

Glauco Bertocchi, CISM
Vice Presidente Capitolo ISACA Roma

NOVITA' DAL CAPITOLO

ISACA 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.
L'intenzione è quella di:

- avvicinare le community nazionali di **ISIPM** e **ISACA**
- ampliare le aree di interesse delle due community
- favorire lo scambio di esperienze e conoscenze
- aumentare il grado di formazione e di competenza nelle tematiche di interesse delle due organizzazioni
- organizzare congiuntamente eventi e/o webinar di "Project Management" e ICT Security Management, per sensibilizzare i propri soci sull'importanza di tali discipline e delle relative metodologie e tecniche.
- sviluppare percorsi formativi congiunti, che uniscano la formazione per le certificazioni di **ISACA (CSX® fundamentals**, **CSX-P**, **CISA®**, **CISM®**, **CGEIT®** e **CRISC®)**, a quella per la certificazione **ISIPM-Base®** e alla qualificazione **ISIPM-Av®** di **ISIPM** (1° e 2° livello di certificazione PM). L'obiettivo è fornire le competenze organizzative, tecniche, ed operative in materia di **Cyber-Security,** insieme alle conoscenze di **Project Management**, utili e necessarie per coloro che partecipano a progetti in vari ruoli o intendono qualificarsi.
- sviluppare e sostenere gruppi di lavoro congiunti, per studiare e creare nuove opportunità, che possono avvicinare sempre di più le due discipline, su obbiettivi comuni.

Informiamo i Soci e i followers di ISACAROMA che, a seguito delle disposizioni volte a contrastare la diffusione del virus COVID-19 (Coronavirus), abbiamo dovuto rinviare lo svolgimento dei consueti seminari in presenza.

Abbiamo quindi predisposto lo svolgimento di eventi on-line a partire da Aprile. 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

Riprenderemo gli eventi in presenza appena sarà possibile.

Vi terremo informati, per il momento vi auguriamo buona lettura!

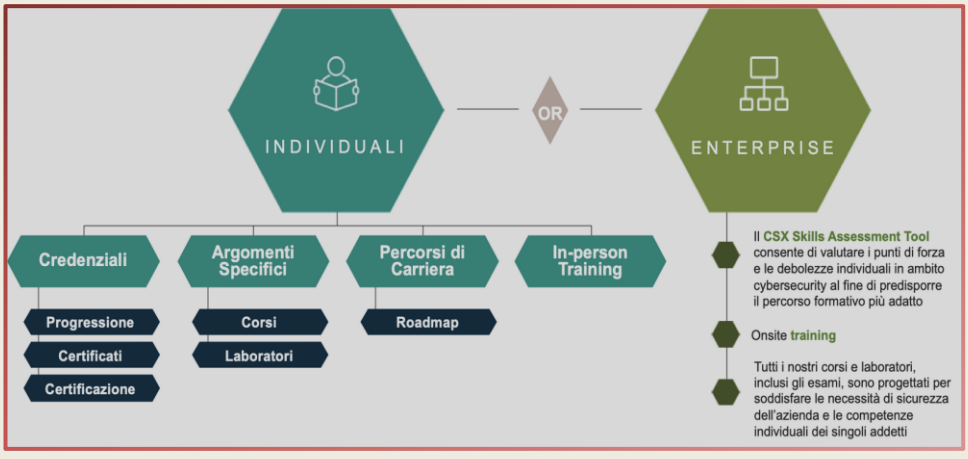
ISACA Roma ha attivato il percorso, teorico e pratico con esercitazioni, per ottenere la certificazione "CSX Practitioner Certificate". Il capitolo di Roma è uno dei pochi in Europa e nel mondo ad aver completato l'iter che consente di erogare lezioni anche on-line e di fornire agli studenti la possibilità di esercitarsi con 70 laboratori virtuali.
CSX-P è stato introdotto da ISACA nel 2015 certificazione indipendente dai fornitori e basata sulle abilità a risolvere problemi, per i professionisti dell'information security e cybersecurity. CSX-P richiede ai candidati di dimostrare le proprie capacità nella cybersecurity in un ambiente dinamico e virtuale, cimentandosi su scenari attuali di cyber security, e non semplicemente superare un esame con domande a risposta multipla.
È la sola certificazione completa basata sulle performance individuali nel settore che verifica l'abilità del candidato di svolgere compiti tecnici nelle 5 funzioni di sicurezza definite dal framework NIST – identify, protect, detect, respond and recover. Ai candidati è richiesto di mettere in pratica le competenze acquisite sulla cybersecurity e dimostrare di possedere le abilità necessarie per reagire a un ambiente di minacce cyber sempre più aggressivo e vario.
CSX Practitioner Certificate consiste nel:
1. risolvere i compiti presenti in 10 laboratori virtuali
2. superare l'esame
3. dimostrare di possedere i requisiti per la certificazione (esperienza pluriennale, possesso di ulteriori certificazioni).
Sono disponibili due tipologie di laboratori virtuali:

- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori indipendenti e utilizzabili off-line.

È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi
Il partecipante svilupperà competenze pratiche sulla cybersecurity oltre a una solida base teorica, il 50% di tutti i corsi comprende degli esercizi pratici di laboratorio in un **cyber ambiente virtuale**. Nello stesso tempo si approfondiranno le tecniche per rispondere agli attacchi e recuperare dati e sistemi in caso di disastro, in particolare:

- Network evaluation
- Vulnerability analysis
- Malware & incident detection
- Incidence reporting
- Safeguard implementation

L'offerta di corsi CSX è molto varia e modulare, ciò consente anche un approccio graduale e focalizzato su specifici ambiti (penetration e vulnerability, analisys, specialist) per consentire una formazione finalizzata qualora necessaria.



Maggiori dettagli sono disponibili qui:
http://www.isacaroma.it/wp-content/uploads/2019/11/CILLI-CSX_Training_Options_IT.pdf
ISACA Roma
- **Segreteria Corsi**
- **Tel. +39 375 599 1500**
- **cybersecurity@isacaroma.it**

www.csxp.it

EVENTI PASSATI

WEBINAR del 10 luglio 2020

"MITRE ATTACK FRAMEWORK: UNO STRUMENTO DA CONOSCERE"

Relatore: ing. Antonio Forzieri

Laureato in Ingegneria delle Telecomunicazioni al Politecnico di Milano, dove è docente nel corso "Mobilità e Sicurezza delle reti"..

In Splunk Forzieri ricopre il ruolo di leader per l'offerta Cyber Security per EMEA. In precedenza, Antonio ha lavorato per Symantec dove ha ricoperto il ruolo di leader per l'offerta Cyber Security a livello EMEA inizialmente e a livello Global successivamente supportando clienti nella realizzazione di complesse iniziative in ambito Cyber Security che vanno dalla costruzione/evoluzione di Cyber Defense Center fino all'implementazione di Programmi di Cyber Intelligence per clienti pubblici e privati. Prima dell'esperienza in Symantec Forzieri ha lavorato per altre aziende italiane con incarichi svolti in tutta EMEA dove si è occupato di diverse tematiche tra le quali Compliance, Endpoint Security, Data Loss Prevention, Encryption, Ethical Hacking, Analisi Frodi, oltre ad attività di formazione in ambito Security. Tra le attività svolte, Forzieri supporta organizzazioni pubbliche e private in caso di attacchi informatici e frodi.

Dal suo primo rilascio il framework ATT&CK del MITRE ha suscitato moltissimo interesse all'interno della comunità di Cyber Security, fornendo un terreno comune sia per il Blue Team che per il Red Team. Ma cos'è esattamente il ATT&CK, e cosa possiamo farci all'interno della nostra organizzazione?

ATT&CK, come ogni framework, possiede moltissime potenzialità e alcune limitazioni che è bene conoscere prima di poterlo utilizzare al pieno delle sue possibilità. Durante questa sessione discuteremo, che tipo di gap abbia colmato il framework e come, attraverso il suo utilizzo, sia possibile migliorare complessivamente la security posture aziendale. Vedremo inoltre come molti prodotti implementino il framework al proprio interno in modo tale da semplificarne la messa in opera operativa e beneficiarne dei contenuti.

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

PROSSIMI EVENTI

WEBINAR del 24 luglio 2020

"EVOLUZIONE DELLA DIGITAL FORENSICS PROFESSIONALE DALL'ANALISI POST MORTEM ALLA LIVE FORENSICS: EVOLUZIONE PRATICA"

Relatore: Massimiliano Graziani

Dopo aver prestato servizio dell'Aeronautica Militare ha seguito la sua vocazione per l'informatica e nel 1992 ha fondato la Cobra Soft, azienda di sviluppo software con la quale ha colto moltissimi primati in ambito di Hacking & Countermeasures, come ad esempio il primo test comparativo sugli antivirus pubblicato in Italia. Dal 2005, si è dedicato completamente agli aspetti della sicurezza, fondando insieme ad altri il capitolo italiano dell'OWASP. Come dipendente ha svolto il ruolo di Manager di area sulla sicurezza IT, in varie aziende di informatica. Ha quindi fondato la sua attuale azienda CYBERA SRL. Dal 2005 ha iniziato una lunga collaborazione, che prosegue con sempre maggiore intensità, con le Procure e Forze dell'Ordine in ambito della Computer Forensics. Socio fondatore del capitolo italiano dell' International Information Systems Forensics Association (IISFA), e dell'Osservatorio Nazionale Informatica Forense (ONIF), E' in possesso delle seguenti certificazioni internazionali: CIFI (Certified Information Forensics Investigator rilasciata da IISFA), CFE (Certified Fraud Examiner rilasciata da ACFE), ACE (AccessData Certified Examiner rilasciata da AccessData), OPSA (OSSTMM Professional Security Analyst rilasciata da ISECOM), CIFIP (Certified Forensic Investigation Professional rilasciata da IICFIP) e CDFP (Certified Digital Forensics Professional rilasciata da IICFIP).
Docente in materia di Digital Forensics Pratica presso Scuola di Polizia Tributaria della Guardia di Finanza, Università La Sapienza Roma (Corso Informatica Giuridica con prof. Aterno), Università LUMSA Roma (Corso Diritto Penale dell'Informatica con prof. Zanotti), Ha svolto e svolge continuamente numerosi corsi e seminari presso le FF.OO , organismi giudiziari, università

Il webinar illustra l'evoluzione dello stato dell'arte vissuta da chi opera professionalmente in quest'ambito.

1) Riepilogo delle regole fondamentali

2) Accenni alla ISO27037

3) Evoluzione degli strumenti hardware professionali

4) Evoluzione degli strumenti software professionali

5) Live Forensics e Sniper Forensics

6) Qualche esempio pratico

7) Domande e risposte

STIAMO ORGANIZZANDO UN WEBINAR PER IL GIORNO 11 SETTEMBRE

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

SUPERCOMPUTER EUROPEI HACKERATI: CHI C'È DIETRO?

20 luglio 2020 – Nel maggio scorso sono apparsi alcuni articoli in cui si leggeva che diversi supercomputer europei (almeno dodici) sono stati hackerati, l'accesso disabilitato, e si è dovuto procedere al loro spegnimento per ripristinarne le condizioni di sicurezza. Sembra che lo scopo degli attaccanti fosse quello di cercare di sfruttare le enormi potenzialità dei supercomputer per "minare crypto currency".
(source: https://www.difesaonline.it/evidenza/cyber/supercomputer-europei-hackerati-chi-c%C3%A8-dietro)

INTELLIGENZA ARTIFICIALE E GDPR SONO COMPATIBILI, MA SERVONO NORME PIÙ CHIARE: LO STUDIO

20 luglio 2020 – Il GDPR, pur non menzionando l'IA, fornisce principi generali rilevanti anche per questa tecnologia. Tuttavia, secondo un recente studio, andrebbe chiarito meglio come questi principi possano applicarsi ai sistemi di IA. Ecco le azioni che servono.
(source: https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-e-gdpr-sono-compatibili-ma-servono-norme-piu-chiare-lo-studio/)

USA, HACKER CINESI A CACCIA DEL VACCINO DOPO AVER GIÀ SPIATO SOCIETÀ DI TUTTO IL MONDO

21 luglio 2020 - Due hacker cinesi hanno rubato segreti commerciali da tantissime società in tutto il mondo per un valore di centinaia di milioni di dollari. E ora sarebbero in azione per sottrarre i risultati delle ricerche sul vaccino anti-Covid. Ovunque sia. Il Dipartimento di Giustizia americano accusa i due cybercriminali di hackeraggio, fa sapere l'Associated Press.
(source: https://www.repubblica.it/esteri/2020/07/21/news/usa_hacker_cinesi_a_caccia_del_vaccino_dopo_aver_gia_ficcato_il_naso_in_societa_di_tutto_il_mondo-262554297/)

GOVERNANCE UNICA SUI DATI PUBBLICI, LA PROPOSTA DI AGID

21 luglio 2020 – Per l'Agenzia serve un organismo di controllo ad hoc. Ciasullo: "Bisogna trovare un equilibrio tra le richieste di dati da parte delle imprese e l'offerta della PA".
(source: https://www.corrierecomunicazioni.it/pa-digitale/governance-unica-sui-dati-pubblici-la-proposta-di-agid/)

7 VPN SERVICES LEFT DATA OF MILLIONS OF USERS EXPOSED ONLINE

21 luglio 2020 – vpnMentor experts reported that seven Virtual Private Network (VPN) recently left 1.2 terabytes of private user data exposed to online.
(source: https://securityaffairs.co/wordpress/106181/data-breach/7-vpn-data-leak.html)

CORSI ISACA

L'ATTIVITÀ FORMATIVA DI ISACA ROMA NON È SOSPESA!

I CORSI SONO EROGATI IN MODALITÀ ONLINE

CISA Certified Information Systems Auditor – An ISACA Certification
CISM Certified Information Security Manager – An ISACA Certification
CGEIT Certified in the Governance of Enterprise IT – An ISACA Certification
CRISC Certified in Risk and Information Systems Control – An ISACA Certification

LA NUOVA CERTIFICAZIONE CSX-P (CYBERSECURITY PRACTITIONER)

Per ulteriori informazioni visitare il sito dedicato alla certificazione CSX-P (www.csxp.it).

SETTEMBRE/DICEMBRE 2020: ULTERIORI INFORMAZIONI NELLE SEZIONI SPECIFICHE DI QUESTO SITO

Corsi a calendario	Durata/ gg	Città	I° Data	II° Data
CSX	3	on line	16-17-18 settembre	1-2-3- dicembre
CISM	5	on line	21-22-23-28-29 settembre	19-20-21-26-27 ottobre
CISA	6	on line	7-8-9-12-13-14 ottobre	18-19-20 -25-26-27 novembre
CGEIT	5	on line	2-3-4-12-13 novembre	-
CRISC	5	on line	5-6-9-10-11 novembre	-
CSX-P	6	on line	19-20-21-26-27-28 ottobre	9-10-11-15-16-17 dicembre

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 ultra decennale 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**

SAPIENZA
UNIVERSITÀ DI ROMA

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

http://www.isacaroma.it/

Social Media

Una nuova Certificazione ISACA **Certified Data Privacy Solutions Engineer** si è aggiunta alle esistenti

I soci Isaca possono accedere ad un percorso semplificato di certificazione durante il periodo di early adoption. Info al sito *https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer*

ANCHE QUESTO ANNO LA NEWSLETTER DI ISACAROMA VA IN VACANZA.
CI RIVEDREMO A SETTEMBRE

BUONE VACANZE A TUTTI

Foto Silvano Bari