Newsletter

ANNO 2020 N. 06 GIUGNO 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

Data Centered Approach

Rimettere il dato al centro per garantire Data Management e Data Protection, evitare la shadow IT e i dark Data e favorire la cultura dei dati digitali mediante Data Literacy.

Quante volte avete sentito la frase "il dato è potere" oppure "viviamo nell'era dei dati" o anche "il tesoro nascosto nei dati"? Qualcuno parla addirittura di "guerra dei dati" con riferimenti agli usi impropri ai fini di marketing personalizzato e controllo della popolazione.
L'era digitale e la conseguente numerosità, tipologia e qualità dei dati che produce, ha generato l'esigenza di una **corretta gestione e protezione dei dati digitali** ed ha aperto la strada alle tecnologie dei Big data. Ha inoltre evidenziato il problema della **Shadow IT e dei Dark Data** (letteralmente dati oscuri) ossia tutte quelle applicazioni e database di dati correlati, che sono "scivolati nel dimenticatoio" dei data center o dei sistemi IT, perché non più utilizzati e soppiantati da nuovi sistemi, ma mai cancellati o deduplicati, o di cui addirittura sono pagate periodicamente licenze del tutto inutili. Ma soprattutto in ambito sicurezza informatica, questi stessi "**dati abbandonati e in disuso**" non sono più protetti e tutelati, e sono quindi appetibilissimi per gli attaccanti, insieme ai **dati finanziari**, a quelli relativi alle **credenziali di accesso** e naturalmente ai **dati personali**. **Tutti questi** tipi di **dati insieme**, **sono** diventati **il nuovo oro**. Diciamo che parafrasando un famoso detto popolare si potrebbe sinteticamente dire che "**chi trova i tuoi dati, trova un tesoro**"! Naturalmente sono proprio le numerose tipologie di attacchi digitali che consentono di esfiltrare dati e usarli, ad esempio nel furto di identità, per frodi digitali o per criptare i dati per poi chiedere un riscatto per la loro restituzione (tipico degli attacchi con ransomware). Si rende quindi necessario sviluppare un appropriato ripensamento dei sistemi ICT in funzione dei dati, adottando un **ragionato Data Management** e, in funzione delle loro esigenze di sicurezza e tutela, provvedere ad una **significativa strategia di Data Protection**. Non si tratta solo di rivedere i sistemi ICT per introdurre una reingegnerizzazione che preveda un "Data lake" al centro e tutti i servizi IT e di security ICT al contorno, come una enorme "cipolla digitale". Il dato deve essere protetto sia quando è "at rest" sia "in transit", ovvero, sia quando è fermo, che in

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

movimento durante le trasmissioni. Questo comporta anche prevedere protezioni per ambienti ibridi e distribuiti che possono essere costituiti da: porzioni di ICT on-site in datacenter tradizionali, porzioni in cloud e da tutte le tipologie di endpoint connessi sia dall'interno che dall'esterno della rete aziendale. Uno scenario di questo tipo non è così distante dalla realtà. Si pensi infatti alla recente emergenza pandemica ed alla conseguenza di un utilizzo massivo di smartworking da ogni casa, verso sistemi aziendali a volte resi accessibili da remoto in modo frettoloso o improvvisato, emergenziale e non sempre ottimale. Nella fretta di implementare lo smartworking le organizzazioni hanno esposto i loro asset online, rendendosi ancor più vulnerabili agli attacchi informatici. È accaduto per i server di posta e per alcune risorse rese accessibili da Web. (fonte check Point). L'emergenza COVID ha generato mille miliardi di bit al secondo (fonte Veritas) con la produzione di un traffico dati che ha rischiato di far crollare le connessioni nazionali. Ogni azienda che volesse perseverare nello smartworking dovrebbe sapere come gestire e proteggere i dati anche a distanza. È necessario stilare policy orientate alla Data Management e Protection per stabilire i requisiti di compliance a cui attenersi. In funzione di questi è necessario indicare la corretta modalità di archiviazione dei dati e il loro trattamento protetto durante le trasmissioni, evitare che le informazioni passino su dispositivi e supporti non protetti e determinare quando i dati sono considerati non affidabili e non utilizzabili. Infine, si rende necessario sviluppare piani di emergenza per gli accessi da remoto e rivalutare periodicamente la strategia di gestione dei dati e della loro protezione per individuare le lacune e pianificarne la risoluzione.

A livello dei singoli e dei cittadini invece, i fatti di cronaca evidenziano tre aree di intervento: **Data Literacy** ovvero l'alfabetizzate delle persone in materia di dati affinché possano leggere, capire, interrogare e comunicare attraverso i dati; **un nuovo Digital Social Contract** che oltre al GDPR, il regolamento generale sulla protezione dei dati promosso dall'Unione Europea e al **Contract for the Web Project** di Sir Tim Berners-Lee, possa portare alla definizione di un quadro normativo preciso da seguire (Fonte Qlik). In ultimo, la **creazione di una cultura e di una consapevolezza (awareness) in merito alla sicurezza dei dati** che insegni alle persone come tutelarli, come salvarli nei back-up, proteggerli con la crittografia e abbassare quel triste primato di circa 6 italiani su 10 che continuano a perdere dati importanti. Il dato emerge da un "sondaggio per analizzare i comportamenti degli italiani in fatto di back up e salvaguardia dei dati" (Fonte world back-Up day). Pur crescendo la consapevolezza dell'importanza della prevenzione (91%), le persone continuano a incappare in errori e per non curanza mancano di adottare prassi di sicurezza basilari. Un ulteriore disgraziata conseguenza è la maggiore vulnerabilità agli attacchi di ransomware contro il quale il ripristino di back-up recente, consente spesso di vanificare gli sforzi dell'attaccante. Un altro dato che sorprende è l'utilizzo superficiale delle chiavette USB che, introdotte nei più variegati gadget, comportano una gestione incauta delle informazioni potenzialmente sensibili contenute al loro interno, con ovvie conseguenze sulla sicurezza. Ancor una volta interventi di awareness sui singoli e l'adozione di policy da parte delle aziende sono i mezzi più adatti per insegnare l'uso corretto delle chiavette e l'adozione di quelle crittografate. Il tema della **formazione a compensazione del divario delle competenze in ambito dati e loro sicurezza** è più ampio di quanto non sembri. Infatti, dalle decisioni prese in emergenza dai livelli decisionali di alcune organizzazioni è stato possibile dedurre quanto estesa sia la platea di manager che non possiedono competenze digitali forti, o addirittura rilevanti e men che meno in ambito sicurezza informatica e data protection. Questo inficia sia la capacità di dare il buon esempio al resto della popolazione aziendale, che la capacità decisionale per le iniziative di crescita future e inoltre impedisce di affrontare i problemi di sicurezza informatica in modo corretto e rilevante (fonte: report annuale Gartner 2019 CEO e Senior Business Executive Survey). Anche lo studio "The Human Impact of Data Literacy" condotto nell'ambito del Progetto Data Literacy, ha rilevato un divario tra le aspirazioni delle organizzazioni di essere guidate con scelte basate sui dati e la capacità dei dipendenti di creare valore di business dai dati stessi. Solo il 25% dei dipendenti intervistati si ritiene pienamente preparato, inoltre nel campione il 37% dei dipendenti si fida maggiormente delle proprie decisioni quando sono basate sui dati mentre il 48% prende decisioni in base all' "istinto". Eppure, non

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

tutti sanno che esiste anche la certificazione di Data Literacy, che sebbene gestita da un'azienda, la Qlik, è la prima nel suo genere. Attorno a questo concetto è nata anche nel 2018 una classificazione delle aziende (il Data Literacy index) che classificava il valore delle società, in base alla disponibilità dei dati necessari e alla capacità di utilizzarli nel processo decisionale.

A conti fatti l'estrema sintesi di tutte le evidenze discusse sembra poter essere condensata in tre azioni:

1. Rendere la sicurezza del dato (data protection) una priorità strategica in tutte le decisioni aziendali.
2. Aumentare la consapevolezza di tutto il personale riguardo la sicurezza informatica e il data management e protection.
3. Implementare un approccio proattivo che includa soluzioni preventive di sicurezza informatica per la data protection e management in ogni condizione e posizione del dato. A tal fine si può prevedere, tra l'altro, l'utilizzo di tecnologie di Intelligenza Artificiale (A:I.) come ad esempio reti neurali specializzate per il data protection.

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.

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.

Seguiteci nei prossimi giorni, così sarete sempre aggiornati e potrete scoprire tutte le attività e le novità in arrivo.

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

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

Speriamo, soprattutto per il bene del nostro paese, che questa situazione emergenziale finisca presto. Noi saremo pronti a riprendere 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.

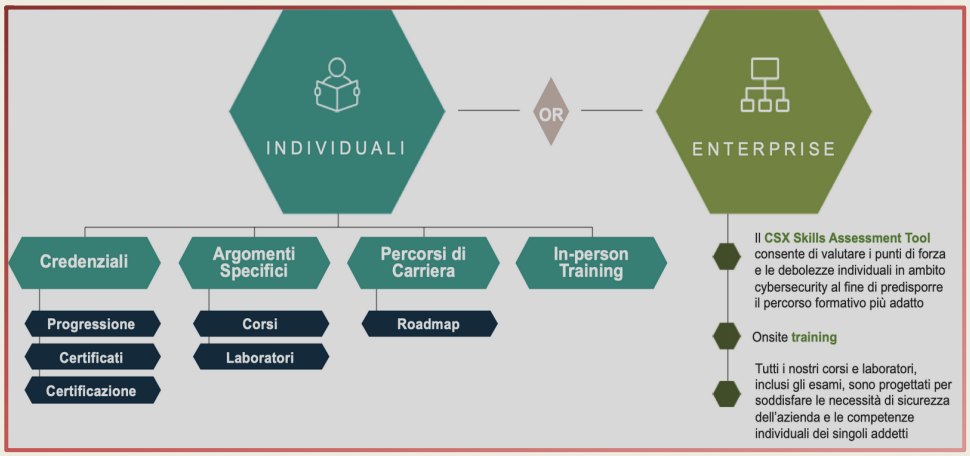
È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi

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

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

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 05 giugno 2020

"EVOLUZIONE DEL RISK MANAGEMENT E RISK QUANTIFICATION"

Relatore: Alberto Piamonte

Una lunga carriera nel mondo ICT con significative esperienze internazionali. Istruttore, Implementor ed Assessor COBIT5.

É uscito recentemente un testo sulla sicurezza informatica *(How to measure anything in Cybersecurity Risk).*

Il testo parte in modo provocatorio ponendosi la seguente domanda: *"Non è che il maggior rischio per la sicurezza informatica sia proprio il modo con il quale la affrontiamo ?".*

I due autori, esperti rispettivamente di tecniche di misurazione e decisionali (Hubbard) e di GRC (Seiersen), ridimensionano la validità e utilità delle tradizionali matrici "Impatto-Probabilità "sostituendoli con metodi quantitativi di semplice applicazione pratica e scientificamente provati.

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

WEBINAR del 15 maggio 2020 **"HOW TO DEFINE AND BUILD THREAT INTELLIGENCE CAPABILITY"**

Relatori: prof. ing. Claudio Cilli (Recognised international authority in the areas of National Security and Intelligence, company protection, information systems security and compliance, with over 25 years of experience. Adjunct Professor at Rome University. CIA, CISA, CISM, CGEIT, CRISC, CISSP, CSSLP, HCISPP, M.Inst.ISP. President of the ISACA Rome (Italy) Chapter)

What is "threat intelligence"? A term overused and ill-defined! What is required to create a true threat intelligence capability, and how does this relate to the nirvana of cyber situational awareness?

During this talk, we will: Define "threat intelligence", distinguishing between threat data and how this can be processed into "intelligence". Discuss some of the data sources (open and closed networks), how organisations are beginning to share more data, and the benefits of incorporating threat data into correlation systems. Explain why data must first be contextualised and ranked before it becomes "intelligence". Argue why this is difficult to automate effectively, and the role your security staff have in operationalising the output. Continue to describe the term "cyber situational awareness", referencing literature and movies in a fun way to explain how this is achieved and why it is important. Show how this enables organisations to achieve an almost unconscious heightened level of security preparedness.

- *Understanding the requirements for threat intelligence*
- *Providing a template for a security organisation wishing to create an intelligence function*
- *How to progress towards "cyber situational awareness"*

Articulate the need for careful investment in staff, not just technology, in order to benefit from threat data.

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.
Per ora possiamo anticipare che stiamo programmando 2 webinar per il prossimo mese di Luglio, quanto prima, tramite i consueti canali, annunceremo le date.

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

LE PRINCIPALI NOTIZIE

L'ATTACCO INFORMATICO CONTRO L'AUSTRALIA

19 giugno 2020 – Va avanti da mesi, sta colpendo istituzioni pubbliche e private e il primo ministro Scott Morrison ritiene che ci sia dietro un paese straniero (molti pensano alla Cina).

(source: https://www-ilpost-it.cdn.ampproject.org/v/s/www.il-post.it/2020/06/19/australia-attacco-informatico/amp/?usqp=mq331AQFKAG-wASA%3D&amp_js_v=0.1#referrer=https%3A%2F%2Fwww.google.com&amp_tf=Da%20%251%24s&ampshare=https%3A%2F%2Fwww.ilpost.it%2F2020%2F06%2F19%2Faustralia-attacco-informatico%2F)

CYBER SECURITY, SCOPERTA VULNERABILITÀ 0-DAY SU DISPOSITIVI SOHO NETGEAR

17 giugno 2020 – Gli esperti di cyber security di Yoroi-Cybaze: scoperta vulnerabilità 0-day su dispositivi SOHO Netgear. Un attaccante può eseguire codice arbitrario nel dispositivo bersaglio prendendone il controllo senza autenticazione. Inoltre, al momento non c'è una patch

(source: https://www.difesaesicurezza.com/cyber/cyber-security-scoperta-vulnerabilita-0day-su-dispositivi-soho-netgear/)

LOTTA ALLE FAKE NEWS: DAL DOCUMENTO DELL'UE AL LAVORO DELLE INTELLIGENCE INTERNAZIONALI

17 giugno 2020 - Ora che è iniziata la **fase 3 dell'emergenza coronavirus** (in vigore dallo scorso 15 giugno con la pubblicazione del DPCM contenente le disposizioni per il periodo fino al prossimo 14 luglio), possiamo portare a casa un'importante lezione che deriva in maniera diretta da tutti gli alert arrivati nel bel mezzo della pandemia: le **fake news**.

(source: https://www.cybersecurity360.it/cybersecurity-nazionale/lotta-alle-fake-news-dal-documento-dellue-al-lavoro-delle-intelligence-internazionali/)

IL NUOVO CSIRT E LA GESTIONE CENTRALIZZATA DELLA DIFESA CYBER: QUALI VANTAGGI

29 maggio 2020 – Istituito presso il DIS (Dipartimento delle Informazioni per la Sicurezza), lo CSIRT costituisce il centro di coordinamento delle attività relative alla prevenzione e alla gestione delle minacce e degli incidenti cyber in Italia e ha quindi un ruolo nevralgico nel monitoraggio della difesa cyber. Ecco con quali vantaggi.

(source: https://www.cybersecurity360.it/cybersecurity-nazionale/il-nuovo-csirt-e-la-gestione-centralizzata-della-difesa-cyber-quali-vantaggi/)

GDPR E DIRETTIVA NIS: ECCO PERCHÉ SONO COLLEGATI E COMPLEMENTARI

11 maggio 2020 – I **beni aziendali** più preziosi e, al tempo stesso, più vulnerabili sono i **dati e** le **infrastrutture**. Con l'obiettivo di proteggere tali beni – informazioni, dati dei dipendenti, know-how dell'azienda, reti informatiche e sistemi informativi che permettono di erogare servizi – l'**Unione Europea**, nel 2016, ha pubblicato **due normative** che gli Stati Membri hanno recepito o stanno ancora recependo.

(source: https://www.lumi4innovation.it/gdpr-direttiva-nis-ecco-perche-sono-collegate-e-complementari/)

INTELLIGENZA ARTIFICIALE ALLA SFIDA HATING: BENE MA NON BENISSIMO

17 giugno 2020 – Cantieri aperti in tutto il mondo sulle tecnologie anti-odio online. In prima linea i team di ricerca che utilizzano sistemi di AI in grado di individuare su miliardi di post e messaggi le parole bersaglio. Prossimo step il riconoscimento del "tono" contenutistico: ma la strada è ancora lunga.

(source: https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-alla-sfida-hating-bene-ma-non-benissimo/)

CORSI ISACA

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

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

CORSI CISA, CISM, CGEIT E CRISC!

COME IMMAGINATE L'EMERGENZA COVID-19 E LE CONSEGUENTI RESTRIZIONI NORMATIVE HANNO PORTATO AL RINVIO A NUOVA DATA DEI CORSI DI ISACA ROMA. STIAMO VALUTANDO COME SOPPERIRE NEL MIGLIOR MODO POSSIBILE.

CISA CISM CGEIT CRISC

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**

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

http://www.isacaroma.it/

Social Media

SAPIENZA
UNIVERSITÀ DI ROMA

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