AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2018	N. 01/2018	FEBBRAIO 2018

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

Cari Associati,
apriamo il nuovo anno con una bella notizia: abbiamo ripristinato la Newsletter ai Soci, che mancava dalla fine del 2013.
Nel frattempo il quadro della protezione delle infrastrutture critiche ha visto l'emanazione della Direttiva NIS e di norme nazionali per la definizione dell'architettura di sistema sulla cyber protection.
Salutiamo la nomina del Prof. Baldoni a Vice Direttore del DIS per la cyber security e auguriamo in bocca al lupo a tutta la squadra che lavorerà su questi temi.
Nell'ultimo biennio AIIC ha:

1. Pubblicato due saggi: le Guidelines for "Critical Infrastructures Resilience Evaluation" e for "Community Resilience Evaluation".
2. Realizzato otto Colloquia, eventi che rappresentano uno dei fattori distintivi di AIIC, in quanto si tratta di incontri volti allo scambio di esperienze tra i diversi attori operanti nel mondo delle Infrastrutture Critiche e nei quali si affrontano le tematiche organizzative, normative, economiche e tecnologiche in ambito di protezione delle Infrastrutture Critiche
3. Partecipato a pubblicazioni, citiamo per esempio il libro bianco sulla cyber security che verrà presentato il prossimo 6 febbraio a Milano
4. Partecipato a numerosi eventi e convegni, citiamo per esempio il convegno della Fondazione ICSA di novembre 2017 sulle aziende italiane di cyber security, un convegno nato dalla necessità di combattere il crimine informatico in un settore di vitale importanza per l'interesse nazionale e la protezione delle infrastrutture critiche.

Nel corso del 2018 contiamo di:

1. pubblicare, nei primissimi mesi dell'anno, i risultati dei Gruppi di Lavoro avviati nel 2017, in particolare:
   a. Big Data Analitcs and Critical Infrastructures Resilience,
   b. Cybersecurity Framework for Supply Chain
   c. Cyber Risk Insurance;
2. proseguire le attività del Gruppo di Lavoro in materia di Security Awareness;
3. proseguire i Colloquia;
4. aggiornare lo statuto dell'Associazione affinché consenta una maggiore governabilità e una migliore fruibilità dei servizi dell'Associazione medesima da parte dei soci.

Il 2018 inizia, dunque, per la nostra Associazione con fatti concreti, awareness, analisi e visioni di dettaglio sui temi caldi che affronteremo, come singoli professionisti e come operatori del settore.
Il Consiglio Direttivo ritiene pertanto molto importante raccogliere proposte e disponibilità operative dei Soci per le attività del 2018. Vi invitiamo pertanto fin da subito ad inviare il vostro contributo, segnalando tematiche di specifico interesse da approfondire: segreteria@infrastrutturecritiche.it.
Vi invitiamo anche a confermare la vostra iscrizione entro il 30 marzo 2018 per poter continuare a partecipare alle attività della associazione e ricevere le sue comunicazioni.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

A nome mio personale e del Consiglio Direttivo dell'AIIC, vi ringrazio per la partecipazione alla vita dell'Associazione e vi auguro una buona lettura.

Luisa Franchina (Presidente dell'AIIC)

ATTIVITA' DELL'ASSOCIAZIONE

Tutti I soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso dell'anno sia nelle sessioni "Colloquia" sia in eventi specifici o nei Gruppi di Ricerca. Chi volesse fornire il proprio contributo è pregato di inviare una mail a: segreteria@infrastrutturecritiche.it, specificando in oggetto "Argomenti di interesse". Nelle prossime newsletter provvederemo ad elencare tutti i temi proposti.

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
  - usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
  - costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi ed autonomi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Association for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e

tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).

- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS –** la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza

Partecipazione di AIIC ad eventi nel 2017

- Evento Resilience IBM - Sandro Bologna
- Confindustria, Firenze 13 marzo 2017 – Luisa Franchina : Cybersecurity: tecnologie e strumenti a protezione dei sistemi aziendali ai tempi di Industria 4.0
- Forum CIG - 14 giugno 2017 – Luisa Franchina : La frontiera delle soluzioni tecniche e infrastrutturali (NIS)
- ITASEC Summit Gennaio 2017 – Venezia – Luisa Franchina
- IRASEC Summit Maggio 2017 – Roma – Luisa Franchina
- Boardleaks Milano 21 febbraio 2017 Luisa Franchina
- Agenda Digitale – 14 novembre Roma – Luisa Franchina
- SELTA IC Security – 15 Novembre – Roma – Luisa Franchina
- Fiera Sicurezza – 16 Novembre – Milano – Luisa Franchina
- Endpoint*: "L'importanza della prima frontiera di difesa"* – 29 Novembre 2017 – Roma (AIIC con Lutech & Check Point) – Silvano Bari e Claudio Pantaleo
- ICSA: "*Cybersecurity made in Italy*" – 30 Novembre – Roma – Luisa Franchina

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NEWS E AVVENIMENTI

Lack of encryption in cloud applications rendering enterprises vulnerable – Enterprises are developing and using enterprise applications on a large scale for various purposes, but a lack of encryption, coupled with serious security flaws in such applications, is also rendering enterprises vulnerable.
https://www.scmagazineuk.com/lack-of-encryption-in-cloud-applications-rendering-enterprises-vulnerable/article/740996/
Scmagazine 01/02/2018

Forget cyber crims, it's time to start worrying about GPS jammers – UK.gov report
The UK must reduce the dependency of its critical infrastructure and emergency services on GPS technology to mitigate against the potentially disastrous impact of signal jamming, a government report has warned.
http://www.theregister.co.uk/2018/01/31/gps_signal_jammers_critical_infrastructure/
The register 31/01/2018

Cyber Crime e protezione delle infrastrutture critiche. Il ruolo degli organi di Polizia
Focus Cyber Security Energia 21/2018 – Sicurezza informatica, cyber crimine e attacchi a infrastrutture critiche. **Nunzia CIARDI**, Direttore del Servizio Polizia Postale e delle Comunicazioni, fa il punto della situazione in italia e illustra il ruolo del CNAIPIC, cioè il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche.
https://issuu.com/energiamedia/docs/focus_n.21_2018_-_cyber_security_en
Energia Media 30/01/2018

Tecnologie e gestione del rischio: i protagonisti della mobilità integrata –
Il Convegno è stato organizzato a dal Consorzio **NITEL**, unitamente a **RFI, ANAS, ASI**, e con il supporto di **CIFI.**
La mobilità integrata è un'asset imprescindibile per il presente ed il futuro prossimo. In relazione alla problematica RFI, ANAS, ASI e NITEL hanno evidenziato i rispettivi presidi e competenze per quanto riguarda le tecnologie e la gestione del rischio, traguardando un arco temporale medio lungo.
Roma 25/01/2018

Virus, nuovo allarme Mirai: a rischio un miliardo fra telecamere, tv e internet delle cose – Un team di esperti di sicurezza informatica ha scoperto una variante del malware che infetta i processori Arc, molto diffusi. Che possono trasformare in un'arma letale, i dispositivi in cui si trovano, in grado tutti insieme di sferrare attacchi cibernetici di portata globale
http://www.repubblica.it/tecnologia/sicurezza/2018/01/15/news/virus_nuovo_allarme_mirai_a_rischio_un_miliardo_fra_telecamere_tv_e_internet_delle_cose-186554532/
Repubblica 15/01/2018

L'intelligence italiana recluta hacker tra diplomati e laureati. Difenderanno le infrastrutture da attacchi in rete – Internet of things, cloud storage, auto connesse e intelligenze artificiali ci renderanno la vita più semplice, ma porteranno anche nuove minacce: l'Italia si prepara a fronteggiare i rischi di un cyberspace sempre più affollato

http://www.repubblica.it/tecnologia/sicurezza/2018/01/10/news/l_intelligence_italiana_recluta_diplomati_e_laureati_difenderanno_le_infrastrutture_da_attacchi_in_rete-186234629/
Repubblica 10/01/2018

Jump-Starting the Dark Grid - A new project led by Lawrence Livermore National Laboratory aims to use distributed energy resources, such as customer-generated solar power, to enhance the electrical grid's ability to recover quickly from blackouts or cascading outages, such as those following major storms or earthquakes. The work is funded through the U.S. Department of Energy's Grid Modernization Initiative.
In less than three years, researchers will attempt to demonstrate the potential of distributed energy resources, including the energy produced by solar panels on homes, to help restore power to the grid from scratch, an effort commonly known as a black start. The black start process is now done manually using special generators that can provide power to slowly bring other generators back online. This normally takes days, but by using a distributed energy resource management system (DERMS) being developed under the research lab's CleanstartDERMS project, the process may be reduced to about four hours. In addition to improving customer reconnection time, a smarter, more robust and selective communication and control system could reduce grid recovery costs.
https://www.afcea.org/content/jump-starting-dark-grid?utm_source=Informz&utm_medium=Email&utm_campaign=Informz+Email
The Cyber Edge, AFCEA International, february 1, 2018

La relazione annuale del COPASIR al Parlamento – Il COPASIR (Comitato Parlamentare per la Sicurezza della Repubblica) ha inviato al Parlamento la relazione annuale e *Cyber Affairs* e *Formiche.net* hanno potuto visionarla. In essa spunta la preoccupazione per uno scenario caratterizzato dal coinvolgimento attivo di Paesi. Il direttore generale del Dipartimento delle Informazioni per la Sicurezza (DIS), **Alessandro Pansa**, ha rilevato, infatti, che "*il terrorismo cibernetico non rappresenta una minaccia molto pericolosa, al contrario dello spionaggio cibernetico che invece si incarna in attacchi sofisticati, di tipo sia tattico che strategico, prodotti da realtà statuali con grande disponibilità di mezzi e persone*". La relazione riconosce il lavoro svolto dal Governo in campo cyber. Con riferimento al Dpcm Gentiloni di febbraio 2017, si evidenzia che "*mediante una nuova architettura istituzionale si dispone ora di una cornice di regole più chiare e lineari in tema di responsabilità e prerogative sia in ambito politico sia tecnico*".
Il Comitato ha anche posto l'accento su "*l'esigenza di accrescere il volume degli investimenti e delle risorse personali, tecnologiche e finanziarie anche nell'ottica di tutelare il principio della sovranità nazionale nel campo della sicurezza cibernetica*".
Tra i consigli del Copasir ci sono anche la "*creazione di un eco-sistema cyber nazionale*" e la "*formazione di una rete che preveda la collaborazione ed interazione tra settore pubblico, mondo privato ed accademico in modo da rafforzare la cultura della sicurezza cibernetica*". Infine è stata delineata "*la complessità di una situazione storica in cui la nostra intelligence e altri soggetti istituzionalmente impegnati nella difesa dai rischi cibernetici sono chiamati ad un rilevante impegno di innovazione e crescita per fronteggiare la rapida e pressoché ininterrotta evoluzione degli strumenti tecnologici*".
http://formiche.net/2018/02/01/cyber-intelligence-italia-copasir-relazione-annuale/
Formiche.net, 1° febbraio 2018

Industrial cyber security continues to be poor, warns report - Unprotected industrial control systems (ICS) can be found by simply searching on Google or Shodan, according to a research

report UK-based security firm Positive Technologies. This is especially worrying in light of the fact that ICS components left exposed to the public internet is increasing every year, and that these components typically run factories, transport networks, power plants and other facilities. Of the 175,632 internet-accessible ICS components detected, approximately 42% were in the US, followed by Germany with 13,242, France (7,759), Canada (7,371), Italy (5,858) and China (4,285).
http://www.computerweekly.com/news/252434299/Industrial-cyber-security-continues-to-be-poor-warns-report?asrc=EM_EDA_88764354&utm_medium=EM&utm_source=EDA&utm_campaign=20180202_NAO%20delivers%20damning%20report%20on%20delayed%20and%20costly%20DBS%20transformation%20project
ComputerWeekly.com 02/02/2018

Davos: Splintered internet could lead to global economic turmoil - Politicians and business leaders discussed the risks posed by fake news, cyber attacks and artificial intelligence to jobs, political stability and global security, at this year's World Economic Forum in Davos.
The disintegration of the internet could lead to disruption of global economies over the next 10 years, the World Economic Forum (WEF) has warned. The increasing reliance of governments, institutions and individuals on interconnected technology was one of the key risks under discussion by business leaders, politicians, academics and non-government organizations who assembled in Davos, Switzerland last week.
A *WEF study* identified the growing reliance on technology as one of the major risks facing global economies over the next 12 months. Cyber attacks are growing in prominence and rank third in the list of most likely threats, while cyber dependency ranked as the second most significant driver shaping global risk over the next 10 years, according to the WEF's *Global risks report 2018*.
https://media.bitpipe.com/io_14x/io_141387/item_1664871/CWE_300118_ezine_pp28.pdf
ComputerWeekly.com 30 January - 5 February 2018

GDPR (General Data Protection Regulation): l'Italia rischia di essere in ritardo per l'applicazione delle nuove regole Ue sulla privacy che partono il 25 maggio. E, anche se ci sono le elezioni in vista, l'amministrazione deve lavorare per essere pronta in tempo. È l'allarme lanciato dalla commissaria Ue alla giustizia Vera Jourova a 100 giorni dall'avvio del 'General Data Protection Regulation'.

PROSSIMI EVENTI

COLLOQUIA – Il programma 2018 dei "Colloquia sulle Infrastrutture Critiche", realizzati da AIIC in collaborazione con l'Università Roma Tre, inizia con l' evento **"La protezione dei dati personali e le infrastrutture critiche: quali sono i punti di attenzione per una corretta attuazione del Regolamento Europeo GDPR".** È schedulato per **mercoledì 28 marzo 2018** alle ore 14.30 presso la Sala Conferenze del Dipartimento di Ingegneria, in via Vito Volterra 62.
Il tema è di grande attualità, in prossimità del 25 maggio 2018, data alla quale, come già sopra evidenziato, il GDPR sarà definitivamente la nuova normativa di riferimento in campo europeo: in questo "Colloquia" si discuterà, con relatori di spicco in campo nazionale, delle principali novità che dovranno essere affrontate dai titolari dei trattamenti - come ad esempio le attività di

valutazione dei rischi e di gestione dei data breach - con specifico riguardo alle aziende che operano nel settore delle infrastrutture critiche, .
Il programma è in corso di definizione e verrà inviato prossimamente a soci e iscritti alla newsletter.

ITASEC18 Italian Conference on Cybersecurity – La seconda conferenza italiana sulla sicurezza informatica (ITASEC18) è un evento annuale supportato dal Laboratorio nazionale per la cibersicurezza di CINI che mira a riunire ricercatori e professionisti italiani provenienti dal mondo accademico, industriale e governativo nel campo della sicurezza informatica.
Sarà il Libro Bianco sulla Cybersecurity in Italia il "pezzo forte" di questa edizione di ITASEC. Il libro bianco mette in evidenza il punto di vista della comunità scientifica nazionale riguardo l'importanza di perseguire una politica di gestione della minaccia cyber derivante dal processo di trasformazione digitale. Delinea un insieme di ambiti progettuali e di azioni trasversali che la comunità della ricerca ritiene essenziali perseguire nel settore pubblico e in quello privato per mantenere nel tempo la minaccia all'interno di un rischio residuo accettabile. Il Libro bianco è stato scritto da oltre 150 docenti universitari e ricercatori provenienti da oltre cinquanta tra Università e Enti di Ricerca, tra i quali **Luisa Franchina**, Presidente dell'AIIC.
(Milano 6-9 febbraio 2018)

La Cyber Security e difesa delle Infrastrutture Critiche – CIAS Elettronica e Spark Security in collaborazione con NCP Italy Srl (Networking Competence Provider) organizzano il seminario di formazione su "la Cyber Security e difesa delle Infrastrutture Critiche". Il seminario sarà rivolto a Security Manager, IT manager, amministratori di rete, responsabili di CED e tecnici IT nonché di interesse per network design, system integrator e chiunque altro abbia il bisogno di acquisire valide competenze nel settore della sicurezza.
L'evento è patrocinato dall'**AICC**
(Roma 20 o 21 Marzo 2018)

La norma CEI 79-3 sugli Impianti di Allarme Intrusione - Assosicurezza, con il sostegno delle aziende associate che sponsorizzeranno l'iniziativa, promuove presso il CEI (Comitato Elettrotecnico Italiano) un convegno di formazione che prevede un corso tenuto da docenti certificati CEI sulla norma CEI 79-3 "Impianti antieffrazione e antiintrusione", e nel pomeriggio una sessione su case history aziendali. Il convegno, rivolto a Progettisti, Distributori, Installatori, Security Manager e a tutti coloro che lavorano o investono nel comparto sicurezza, intende fornire i principi alla base della progettazione di questi impianti illustrandone nel contempo i sottosistemi componenti (Rivelatori, Centrale e Dispositivi di allarme) ed il quadro tecnico-normativo.
L'evento è patrocinato dall'**AIIC.**
(Milano 15 febbraio 2018)

CRITIS 2018 – La *XIII International Conference on Critical Information Infrastructures Security, CRITIS 2018*, si terrà a Kaunas, Lithuania. L'edizione 2018 della conferenza continuerà la tradizione di presentare ricerche innovative ed esplorare nuove sfide nel campo della protezione delle infrastrutture critiche informatizzate e promuovere il dialogo tra tutte le parti interessate alle CII. L'evento intende riunire ricercatori e professionisti provenienti dal mondo accademico, dagli operatori di CII, dall'industria, dal settore della difesa e dalle organizzazioni governative che operano nel campo della sicurezza delle infrastrutture critiche informatizzate. Come negli anni precedenti, i relatori invitati e gli eventi speciali realizzeranno un programma di contributi di ricerca originali.

L'evento è patrocinato dall'**AIIC.**
(Kaunas, Lithuania, 24-26 settembre 2018)

ACCADUEO –Mostra Internazionale dell'Acqua – L'evento darà voce a tutti gli operatori in grado di trasferire valore ai diversi ambiti che impattano il settore idrico: il civile, l'industriale, l'agricolo. Con un approccio che guarda all'interesse pubblico e al tempo stesso alla costruzione di una filiera industriale tra le più evolute, in grado di dare slancio al settore.
I focus di ACCADUEO 2018:
• *INNOVAZIONE:* sarà sviluppato il percorso novità per consentire alle aziende di poter comunicare e mostrare i loro prodotti sulla stampa specializzata anche internazionale.
• *INTERNAZIONALE*: saranno costruite delle operazioni di networking internazionale con esperti, progettisti, società ed utilities straniere per gli espositori di ACCADUEO.
L'evento è patrocinato dall'**AIIC**
(Bologna 17-19 ottobre 2018)

Incontro di studio su Privacy by Design and by Default – Il Master in "*Responsabile della Protezione dei dati personali: Data Protection Officer e Privacy Expert*" è stato organizzato dell'Università Roma Tre, la quale in collaborazione con l'Associazione DPOInnovation, ha previsto un evento su "*Privacy by design and by default*". L'incontro si terrà il prossimo **15 febbraio 2018** dalle ore **15.00 alle 18.00** presso l'aula 5 del Dipartimento di Giurisprudenza dell'Università degli Studi "Roma Tre", in viale Ostiense 159. Parteciperanno in qualità di relatori l'avv. Lorella Bianchi (Funzionario del Garante per la protezione dei dati personali) e l'avv. Guido Scorza (Studio legale E-lex). L'incontro è aperto a tutti.

Master in Homeland Security – Il giorno **15 febbraio 2018** si aprirà la X edizione del Master universitario di II livello in "*Homeland Security – sistemi, metodi e strumenti per la security e il crisis management*" presso l'Università Campus Bio-Medico di Roma. Il Master mira a formare tecnici e professionisti in grado di elaborare un processo di analisi delle esigenze di sicurezza, identificare contromisure da adottare, progettare e sviluppare soluzioni integrate per ciò che riguarda l'attuazione e la gestione e l'esercizio di procedure e sistemi di sicurezza.
In occasione della giornata inaugurale del Master, si terrà un convegno sulla *security*, aperto a tutti.
Per tutte le info: www.masterhomelandsecurity.eu
Il Master è patrocinato dall'**AIIC.**
(Roma 15 febbraio 2018)

NOTIZIE D'INTERESSE:

Preghiamo I soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali aggiornamenti potrebbe impedire, al socio, la ricezione delle comunicazioni.

Vi ricordiamo che, salvo eventi speciali riservati ai soli soci, la partecipazione ai Colloquia è libera. Inoltre, ogni socio può suggerire un tema, proporsi come relatore o come organizzatore di un Colloquia: suggerimenti e richieste possono essere inviate al coordinatore dei seminari AIIC, il vicepresidente Silvano Bari, all'indirizzo email segreteria@infrastrutturecritiche.it mettendo in oggetto "Colloquia".

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@InfrastruttureCritiche.it

o visitate il sito

www.InfrastruttureCritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Spalato, 11 – 00198 ROMA Tel. +39 06 64003640 Email segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente cliccare questo link: http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter" del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *segreteria@infrastrutturecritiche.it*