La Sicurezza Delle Informazioni Nel Contesto Evolutivo Del Binomio Comunicazione Informatica

La tutela dei dati nel settore salute
Le convenzioni internazionali della navigazione marittima, interna e aerea
YSEC Yearbook of Socio-Economic Constitutions 2020
Ispezioni e sanzioni nel Testo Unico Sicurezza del Lavoro
La serie ISO/IEC 20000. Requisiti, raccomandazioni, suggerimenti
A Common European Law on Investment Screening (CELIS)
Il nuovissimo Codice degli Appalti
L'orecchio di Dio. Anatomia e storia della National Security Agency
La Sicurezza Delle Informazioni Nel Contesto Evolutivo del Binomio Comunicazione-Informatica
con focus su archiviazione e fatturazione elettronica
United States Treaties and Other International Agreements
Telecomunicazioni, criptografia, steganografia, digital watermarking, reti cablate, reti wireless, comunicazioni vocali, protezione dalle intercettazioni. Nel CD Rom allegato programmi per criptografia e steganografia
Accesso non autorizzato
La sicurezza dei domini digitali
Sicurezza delle comunicazioni
Essential Cyber Security Handbook In Italian
Il risk management. Teoria e pratica nel rispetto della normativa
Aggiornato a giugno 2017
Sicurezza delle informazioni
ISO27001/ISO27002: Una guía de bolsillo
Manuale Essenziale di Cyber Security in italiano
guida operativa alla nuova disciplina dopo il D.Lgs. 20 giugno 2016, n. 116 : le responsabilità del dipendente pubblico, la responsabilità dirigenziale e disciplinare del dirigente, l'applicazione delle sanzioni disciplinari ...
Nuovi conflitti tra privacy e salute. Annuario data protection 2020
Compendio per l’attuazione della norma ISO 27001:2013
I nove passi per il successo
Treaty Series 1577
Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001
Prevenire gli eventi avversi nella pratica clinica
Information security: risk assessment, management systems, the ISO/IEC 27001 standard
Cyberworld
7a edizione

Privacy in azienda. Manuale di formazione per titolari, responsabili e incaricati
Nuovi standard sulla sicurezza informatica e regolamento per la protezione dei dati personali: i modelli adottabili e le testimonianze degli addetti ai lavori
Sicurezza delle informazioni: educare l'azienda
Il nuovo Codice degli Appalti e delle Concessioni
Capire, prevenire e proteggersi dagli attacchi della rete
Competenze Digitali per la PA - Termini, definizioni e acronimi
Guida al Codice dell'amministrazione digitale

ALIJAH COHEN

La tutela dei dati nel settore salute
Springer Science & Business Media
Un testo completo e pratico con tutte le informazioni necessarie per imparare a comunicare in massima sicurezza. L'intercettazione, il danneggiamento o la perdita di informazioni durante la trasmissione delle informazioni può infatti produrre dei danni materiali, non materiali ed economici dal punto di vista personale, aziendale e della collettività. La sicurezza delle comunicazioni rappresenta, in sostanza, un settore strategico per la protezione della privacy e per la sicurezza personale, aziendale, nazionale e internazionale. Di qui l'importanza di questo libro che vuole offrire anche al lettore non particolarmente esperto, le nozioni relative a tutti gli aspetti di sicurezza delle comunicazioni, partendo dai concetti di base sino ad arrivare ai concetti più avanzati ed attuali, cercando di semplificare al massimo la trattazione. Il testo è rivolto ai progettisti ed amministratori di sistemi di telecomunicazione, informatici e di sicurezza integrati; agli ingegneri di sistema; agli analisti di sistema; ai security manager; ai responsabili della sicurezza; ai responsabili delle infrastrutture critiche; alle forze dell'ordine; alle forze armate; ai ricercatori e ai tecnici del settore; al personale di sicurezza; agli investigatori privati; agli studenti universitari e a tutte le persone che in qualche maniera hanno bisogno di comunicare in maniera sicura per motivi personali o lavorativi. Nel CD rom allegato sono contenuti dei programmi di utilizzo libero (freeware) per criptografia e steganografia utili per comunicare in maniera sicura e per garantire la riservatezza dei dati e delle informazioni all'interno del proprio computer.
Le convenzioni internazionali della navigazione marittima, interna e aerea
IPSOA
Nasce dalla collaborazione di circa seicento professori che hanno passato almeno un lustro a confrontarsi con le problematiche della figura del preside, un manuale enciclopedico che affronta in modo sintetico ed esaustivo tutti gli argomenti oggetto dei concorsi MIUR. L’inusuale modalità di lavoro di gruppo ha consentito di trattare la materia sia in estensione sia in profondità, rendendo questo manuale uno strumento unico, aggiornato a gennaio 2020.
YSEC Yearbook of Socio-Economic Constitutions 2020 Youcanprint
Logistics has become a strategic factor for development and competition. Terrorist attacks, such as 11th of September 2001 in the USA, have caused the introduction of rules and

procedures, which affect the overall logistics showing the vulnerability of the global economy. This book presents the status of research on dangerous goods transport.

Ispezioni e sanzioni nel Testo Unico Sicurezza del Lavoro IPSOA

Per poter tenere testa a un hacker, bisogna pensare come un hacker. Kevin Beaver, noto esperto nel campo della sicurezza informatica, spiega che cosa motiva gli hacker e che cosa cercano nei nostri device. Ci mette a parte dei segreti del test di vulnerabilità e penetrazione, ci spiega le migliori pratiche di sicurezza e ogni altra cosa che dobbiamo conoscere per bloccare gli hacker prima che provochino problemi alla nostra organizzazione. Impariamo a proteggere i nostri server e i desktop, le applicazioni web, i dispositivi mobili o l'intera rete!

La serie ISO/IEC 20000. Requisiti, raccomandazioni, suggerimenti IT Governance Ltd

La questione della sicurezza dei pazienti e del rischio clinico rappresenta da sempre un problema in medicina, ma è a partire dagli ultimi anni che essa è diventata un ambito prioritario della qualità nei servizi sanitari. La medicina non è una scienza esatta e le cure mediche non sono sempre efficaci e affidabili. La materia è inoltre così vasta e complessa da rendere impossibile agli operatori una conoscenza completa di ogni aspetto; a ciò si aggiunge il fatto che i pazienti non sempre si attengono correttamente alle indicazioni di terapia. La valutazione del rischio e l'analisi degli eventi avversi possono quindi contribuire ad accrescere i livelli di sicurezza degli assistiti, a ridurre l'inappropriatezza delle procedure e a impiegare meglio le risorse umane e tecnologiche. Questo volume, dopo una prima valutazione dello stato dell'arte della sicurezza del paziente in Italia e all'estero, presenta i metodi più diffusi per l'analisi degli eventi avversi nelle diverse specialità (medicina d'urgenza, ostetricia e ginecologia, oncologia, salute mentale, ecc.) e nei servizi di supporto (laboratori analisi, radiologia, trasfusioni, farmaceutica). Sono inoltre esaminati gli incidenti più frequenti in strutture extraospedaliere (come ambulatori di medicina generale, servizi sanitari delle carceri). Quest'opera, caratterizzata da una particolare vastità di argomenti trattati, descrive come contenere il rischio e prevenire gli eventi avversi in sanità, analizzando la natura dell'errore umano e applicando le pratiche di sicurezza più efficaci.

A Common European Law on Investment Screening (CELIS) EPC srl

Cosa vuol dire "La sicurezza delle informazioni nel contesto evolutivo del binomio comunicazione-informatica"? Sostanzialmente che oggigiorno è necessario considerare la sicurezza delle informazioni nell'ottica della comunicazione. Non ci si può esimere dal parlare di comunicazione quando si ha a che fare con la sicurezza delle informazioni. Questo perché le informazioni sono la materia prima della comunicazione, e parlare di sicurezza delle informazioni vuol dire anche parlare di sicurezza della comunicazione stessa. Gli argomenti esposti in questo libro sono tratti, e successivamente elaborati e semplificati, per la maggior parte dalle mie lezioni di "Scritture Segrete" fatte agli studenti del corso di laurea in Scienze della Comunicazione dell'università Insubria di Varese, nella quale sono stato docente negli anni accademici 2007/2008 e 2008/2009. Nello specifico, affronteremo un viaggio alla scoperta della sicurezza delle

informazioni, dell'evoluzione delle tecnologie informatiche in piena sinergia con lo sviluppo della comunicazione e delle sue modalità espressive. Ampio risalto sarà dato inoltre alla crittografia e ai suoi metodi per occultare le informazioni al fine di garantire la sicurezza della comunicazione. Il modello espositivo adottato è orientato a facilitare la comprensione dei concetti generali con esposizioni chiare, semplici, intuitive e con l'apporto di diversi esempi esplicativi. Le nozioni tecniche sono ridotte all'osso e all'indispensabile. Tutto ciò per rendere la sicurezza informatica, i cui concetti sono spesso ostici ai più, comprensibili a tutti e in questo modo sdoganarli dalla stretta cerchia degli esperti del settore, per renderli fruibili anche dai neofiti. Per questo motivo si è preferito esporre pochi concetti basilari, per fare in modo di essere alla portata di tutti. In definitiva, questo é un libro i cui contenuti esulano deliberatamente dagli approfondimenti tecnici, proprio per lasciare spazio ai concetti basilari che, essendo espressi in maniera semplificata, possono essere tranquillamente letti e compresi da una vasta audience che va dalle persone in età adolescenziale sino alle persone più adulte che, anche se poco consone all'utilizzo delle tecnologie informatiche, vogliono comunque comprendere il funzionamento del mondo della sicurezza informatica senza perderne di vista i concetti basilari. Sommario Introduzione Capitolo 1 L'importanza della sicurezza delle informazioni Capitolo 2 Evoluzione delle tecnologie della comunicazione Capitolo 3 Informatica e sviluppo tecnologico nel contesto della comunicazione Capitolo 4 Cosa vuol dire garantire la sicurezza delle informazioni Capitolo 5 Le tipologie di attacco più frequente ai sistemi informativi 5.1 Spoofing di indirizzi IP 5.2 Sniffing di pacchetti 5.3 Shadow server 5.4 Collegamenti hijacking 5.5 Negazione di servizio Capitolo 6 I concetti fondamentali della crittografia 6.1 Che cos'è la crittografia 6.2 Le tipologie di algoritmi per crittografare 6.3 Tecniche crittografiche fondamentali Capitolo 7 Breve storia della crittografia e dei sistemi di scrittura occulta adottati nel tempo 7.1 Cenni storici 7.2 La cifratura di Cesare 7.3 La tabella di Vigenere 7.4 Altre tecniche antiche di cifratura Capitolo 8 Nozioni basilari di crittoanalisi 8.1 Che cos'è la crittoanalisi 8.2 Tipi di attacchi da crittoanalisi 8.3 Tipologie di crittoanalisi Conclusioni Bibliografia/Sitografia Informazioni sull'autore

Il nuovissimo Codice degli Appalti

Lulu.com

In accordance with Article 102 of the Charter and the relevant General Assembly Resolutions, every treaty and international agreement registered or filed and recorded with the Secretariat since 1946 is published in the United Nations Treaty Series. At present, the collection includes about 30,000 treaties reproduced in their authentic languages, together with translations into English and French, as necessary. The Treaty Series, where treaties are published in the chronological order of registration, also provides details about their subsequent history (i.e., participation in a treaty, reservations, amendments, termination, etc.). Comprehensive Indices covering 50-volume-lots are published separately.

L'orecchio di Dio. Anatomia e storia della National Security Agency

Edizioni Guerini e Associati

La comunicazione e l’interazione sociale risultano, oggi, ampiamente basate sul concetto di socialità digitale, con

modalità che stanno radicalmente trasformando il dialogo e gli scambi interpersonali. Gli attori principali della rivoluzione digitale che interessa, a velocità distinte, le varie parti del globo sono le aziende, le pubbliche amministrazioni e gli stessi cittadini. Con la transizione verso il digitale, beni, competenze, capitali intellettuali e risorse stanno rapidamente migrando all'interno di luoghi immateriali, spesso difficili da definire e geo-localizzare. Ciò comporta rischi di diversa natura. Le minacce che interessano la sfera dei domini digitali sono molteplici e asimmetriche, in quanto provengono sia da hacker solitari sia da grandi aziende o Stati organizzati. Quale che sia l'autore di un attacco cyber, gli obiettivi di fondo restano quelli di ottenere un profitto economico, o indebolire il proprio avversario, oppure ancora lanciare un messaggio propagandistico, bellico o terroristico. Lo scopo del presente lavoro, quindi, è stato la ricerca di pareri propositivi ed innovativi che individuino gli interventi organizzativi, procedurali e tecnologici necessari per garantire la sicurezza dei Domini Digitali in Italia. Tali pareri sono stati forniti da rappresentanti di istituzioni, università e ricerca, pubblica amministrazione e aziende private, nell'ambito delle sessioni di lavoro del Gruppo della Fondazione Astrid sulla Sicurezza dei Domini Digitali. Questo volume li raccoglie e li propone al dibattito pubblico.

La Sicurezza Delle Informazioni Nel Contesto Evolutivo del Binomio Comunicazione-Informatica HOEPLI EDITORE

La sicurezza delle attrezzature di lavoro è fondamentale per la prevenzione degli infortuni perché interviene a monte dei processi finalizzati alla sicurezza dell'apparato produttivo. Questo volume si propone di offrire una ricostruzione della normativa che governa l'intero "parco macchine" attualmente esistente in Italia – sia esso nuovo, recente o futuro, oppure vecchio – se, comunque, messo a disposizione dei lavoratori in qualsiasi luogo di lavoro. Si ripercorre quindi l'evoluzione di tale produzione normativa, dall'art. 7 del D.P.R. n. 547/1955 al D.Lgs. n. 626/1994, dal vigente D.Lgs. n. 81/2008 - come modificato dal D.Lgs. n. 106/2009 - fino al D.Lgs. n. 17/2010, che ha recepito la "Direttiva macchine" 2006/42/CE. Questa seconda edizione è arricchita da una guida pratica dedicata prevalentemente alla redazione del fascicolo tecnico, delle "istruzioni" e delle "avvertenze", vale a dire la documentazione che nell'esperienza maturata con la "Direttiva macchine" ha evidenziato particolari criticità. Infine, completa il volume una rassegna della giurisprudenza della Suprema Corte in materia di obblighi e responsabilità per la sicurezza delle "macchine". STRUTTURA I parte - Disciplina delle attrezzature di lavoro 1. Progettazione delle attrezzature di lavoro 2. Fabbricazione e fornitura delle attrezzature di lavoro 3. Installazione delle attrezzature di lavoro 4. Uso delle attrezzature di lavoro 5. Obblighi del datore di lavoro 6. Obblighi dei noleggiatori e dei concedenti in uso 7. Informazione e formazione 8. Le sanzioni II parte - Il decreto di attuazione della "direttiva macchine" 2006/42/CE 9. Il D.Lgs. n. 17/2010: analisi e commento dell'articolato 10. Gli allegati al D.Lgs. n. 17/2010 III parte - Indicazioni operative per la redazione del fascicolo tecnico e delle "avvertenze" sui "rischi residui 11. Guida alla realizzazione del fascicolo tecnico di costruzione delle macchine 12. Guida alle "avvertenze" sui rischi

residui 13. La valutazione dello stress lavoro correlato con le carte di controllo in un’azienda del terziario avanzato Rassegna di giurisprudenza Appendice normativa
con focus su archiviazione e fatturazione elettronica FrancoAngeli
In questo libro (aggiornato nel 2017) si trattano: la sicurezza delle informazioni, i relativi processi di valutazione e trattamento del rischio (con un'ampia parte teorica bilanciata da molti esempi), i controlli di sicurezza. Il testo si basa sulle norme ISO/IEC 27001 e ISO/IEC 27002, secondo interpretazioni maturate durante i lavori di scrittura della norma stessa a cui l'autore ha partecipato. Le appendici riportano brevi presentazioni (sulla gestione degli auditor, sulla certicazione ISO/IEC 27001, sui Common Criteria e sulle FIPS 140) e delle check list (per la gestione dei cambiamenti, l'identificazione delle minacce e i contratti con i fornitori).
United States Treaties and Other International Agreements IPSOA
Il fattore umano, non la tecnologia, è la chiave per fornire un adeguato e appropriato livello di sicurezza in azienda. Dati e applicazioni danneggiati da malware o altri incidenti tecnici, furto o divulgazione dolosa o colposa di informazioni sensibili, sanzioni per mancata compliance a causa di eventi imprevisti, sono inconvenienti nei quali può incorrere un’azienda per colpa di una cattiva gestione della sicurezza delle informazioni al proprio interno. Un programma efficace di Awareness e formazione a livello aziendale è fondamentale per assicurare che le persone comprendano le proprie responsabilità di sicurezza e le policy organizzative, ed è importante perché imparino a usare e proteggere, in modo adeguato, le risorse a esse assegnate. Questo libro è una guida per costruire, attuare e mantenere un programma innovativo e completo di Awareness e formazione. Le linee guida sono presentate in forma di approccio a ciclo di vita: partono dalla progettazione di un programma di Awareness e training; passano poi al suo sviluppo e alla sua implementazione; arrivano infine alla valutazione ex-post del programma stesso. Il libro spiega anche come i manager della sicurezza possono identificare le necessità di Awareness e training, sviluppare un piano formativo e ottenere i finanziamenti adeguati. Questa guida si rivolge ai manager dei dipartimenti Organizzazione, Risorse Umane, Information Technology, Sicurezza e Risk Management. Il successo di un programma di Awareness e training, nonché del programma di sicurezza aziendale, dipende dall’abilità di queste persone di perseguire il comune obiettivo di proteggere le risorse informative aziendali. STRUTTURA 1. La gestione del programma di Security Awareness 2. Come giustificare un programma di security Awareness 3. Pianificare un programma di Awareness 4. La valutazione di un programma di sicurezza 5. Il marketing della sicurezza 6. Principi di base della formazione sui temi della sicurezza delle informazioni 7. Performance ed esperienza di apprendimento 8. Security Awareness e standard di sicurezza
Telecomunicazioni, criptografia, steganografia, digital watermarking, reti cablate, reti wireless, comunicazioni vocali, protezione dalle intercettazioni. Nel CD Rom allegato programmi per criptografia e steganografia Mario Canton
Per chi si occupa di dati, il 2020 doveva essere il solito anno tumultuoso in cui analizzare nuovi databreach, decisioni e

provvedimenti, che effettivamente si sono verificati. Ma il Covid-19 ne ha stravolto l'agenda. Tracciamenti, geolocalizzazioni, anonimizzazione dei dati dei contagi sono solo alcune delle parole che hanno investito il mondo della privacy, e sono diventate prioritarie per quello del data protection e delle tecnologie. Così la pandemia ha toccato le corde sensibilissime della privacy del cittadino-paziente: quelle che fanno vibrare la sfera più intima della salute individuale, da una parte, e quella statale della sanità pubblica, dall'altra. Oggi DPO, avvocati, esperti di diritto delle tecnologie, ma anche capi del personale, direttori e dirigenti di aziende sanitarie pubbliche e private sono direttamente coinvolti in una grande prova di resistenza ed equilibrio: perseguire l'interesse pubblico generale e insieme garantire i diritti del singolo.
Accesso non autorizzato IT Governance Ltd
La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale ed è regolamentata in Europa dal GDPR e, in Italia, attraverso il D. Lgs 101 del 10/08/18, ha abrogato gli articoli del codice per la protezione dei dati personali del D. Lgs. n. 196/2003, con esso incompatibili. Il GDPR promuove la responsabilizzazione (accountability) del titolare del trattamento e l'adozione di politiche e approcci che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. La norma ISO/IEC 27701 è stata emessa per aiutare le organizzazioni a far fronte alla difficoltà che riscontrano per soddisfare il requisito dell'art. 35 del GDPR relativo alla valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali. La norma specifica i requisiti in una forma che si estende alla ISO/IEC 27001, ISO/IEC 27002, ISO 27018 e la serie ISO/IEC 29000 per la gestione della privacy. Il presente libro riprende passo passo i concetti delle norme, sviluppa le prescrizioni e gli approcci ed entra in dettaglio nei concetti approfondendo con esempi pratici e dettagliati il processo di Privacy Risk Management. Il libro è strutturato in modo tale da introdurre il lettore progressivamente nell'argomento. Il valore del libro si percepisce in quanto pratico e operativo. La spiegazione teorica dei requisiti e dei concetti delle norme esposti nei vari capitoli si concretizzano con l'esempio pratico del Caso di Studio studiato appositamente per trasferire il know-how e l'esperienza necessaria ai Titolari e Responsabili di trattamento, ai Risk e Security Manager e a tutti quelli che sono interessati alla privacy e sono costretti ad applicare il processo di Privacy Risk Management nella propria organizzazione per tutelare i diritti e le libertà degli interessati.
La sicurezza dei domini digitali Fazi Editore
100.710
Sicurezza delle comunicazioni FrancoAngeli
Il volume è un utile strumento di formazione e di autoapprendimento per chi opera nel settore salute. Si analizzano il ruolo e gli effetti dell'innovazione su individui ed organizzazioni, si identificano e si valutano le potenziali aree di rischio, i modelli adottabili e i comportamenti da tenere per cogliere le maggiori opportunità offerte dal mutato scenario di riferimento della società dell'informazione. Da un lato si presta attenzione agli approcci adottati dai

nuovi standard per la sicurezza informatica, dall'altro si esaminano le recenti disposizioni normative in materia di privacy e la prossima applicazione del nuovo regolamento europeo per la protezione dei dati personali. Partendo dagli spunti offerti dai diversi attori in vista delle nuove minacce informatiche e delle nuove regole europee, si analizzano i modelli promossi dalle organizzazioni internazionali e si contestualizzano le ultime novità al mutato ambito di riferimento, in particolar modo nel settore salute italiano. Infine si evidenzia come le nuove forme di conformità richieste possono essere intese, oltre che come vincoli, anche come principi fondamentali da adottare nei comportamenti da seguire. Il libro che nasce dall'esperienza sul campo dell'autore, segue un percorso logico per il quale in ogni capitolo sono dichiarati gli obiettivi, forniti i test iniziali di accertamento delle conoscenze, inseriti i punti essenziali che vengono poi esplosi nel libro e, al termine di ciascun capitolo, si verificano le conoscenze acquisite con appositi test.

Essential Cyber Security Handbook In Italian EPC srl

"Competenze Digitali per la PA - Termini, definizioni e acronimi" è un glossario utile alla comprensione di termini e concetti del mondo digitale applicato e gestito nella pubblica amministrazione. Il glossario è allineato alla versione del Syllabus "Competenze Digitali per la PA" curato dal Dipartimento della Funzione Pubblica – Ufficio per l'innovazione e la digitalizzazione" aggiornato nella versione 1.1 a luglio 2020. Il Syllabus descrive il set minimo di competenze che ciascun dipendente pubblico dovrebbe possedere per poter operare in modo consapevole e proattivo il proprio ruolo in una pubblica amministrazione sempre più digitale. Attualmente si compone di 113 conoscenze e abilità organizzate in 11 competenze e 3 livelli di padronanza raggruppati in 5 aree di competenza, si configura come uno strumento "vivo" in quanto oggetto di manutenzione continua per stare sempre al passo con le innovazioni tecnologiche, normative e sociali che interessano il sistema della PA italiana. La piattaforma è disponibile alle pubbliche amministrazioni all'indirizzo: https://www.competenzedigitali.gov.it/

Il risk management. Teoria e pratica nel rispetto della normativa Ayros Editore

La "società dell'informazione" è oggi paragonabile a una piazza virtuale nella quale gran parte delle attività giornaliere viene svolta dal "cittadino digitale". Diffondere la consapevolezza dei rischi, elevando la sicurezza per tutti coloro che navigano, interagiscono, lavorano, vivono in rete e sui social media, diventa quindi un passo fondamentale, non dimenticando le questioni di sicurezza nazionale e l'evoluzione degli scenari internazionali. Ecco allora la necessità di un testo che guidi alla scoperta di questo cyberworld, approfondendo le tematiche centrali di settori chiave quali l'economia, la tecnologia, le leggi. Uno studio interdisciplinare del problema dell'hacking passando per il profiling, le dark network fi no alla cyber law e includendo interessanti analisi puntuali su temi verticali, nello stile di un "white paper".

EPC srl

366.60

Aggiornato a giugno 2017 Apogeo Editore

This book presents the very first, interdisciplinarily grounded, comprehensive appraisal of a future "Common European Law on Investment

Screening". Thereby, it provides a foundation for a European administrative law framework for investment screening by setting out viable solutions and evaluating their pros and cons. Daimler, the harbour terminal in Zeebrugge, or Saxo Bank are only three recent examples of controversially discussed company takeovers in Europe. The "elephant in the room" is China and its "Belt and Road Initiative". The political will in Europe is growing to more actively control investments flowing into the EU. The current regulatory initiatives raise several fundamental, constitutional and regulatory issues. Surprisingly, they have not been addressed in any depth so far. The book takes stock of the current rather fragmented regulatory approaches and combines contributions from leading international academics, practitioners, and policy makers in their respective fields. Due to the volume's comprehensive approach, it is expected to influence the broader debate on the EU's upcoming regulation of this matter. The book is addressed to participants from academia as well as to representatives from government, business, and civil society.

Sicurezza delle informazioni Lulu.com L'opera, che vede la collaborazione di diversi studiosi e professionisti specializzati nel settore, approfondisce la complessa tematica del rapporto fra diritto e nuove tecnologie, privilegiando un approccio di carattere operativo anche se non viene risparmiato spazio ad importanti riferimenti di carattere dottrinario. Grande rilevanza assume la giurisprudenza, spesso decisiva per risolvere le particolari questioni giuridiche sorte con l'avvento della tecnologia. Il libro si suddivide in 4 macroaree: civile, penale, amministrativa e tecnologie emergenti, proprio per evidenziare l'evoluzione che negli ultimi tempi ha contraddistinto la materia, da intendere ormai come comprensiva sia dell'informatica del diritto, che del diritto dell'informatica e dove ormai lo stesso riferimento alla sola informatica appare limitato. Proprio per questo motivo si è ritenuto di affrontare le principali ed emergenti tematiche dell'informatica giuridica: la contrattualistica, la protezione dei dati personali, i reati, la cybersecurity, la digitalizzazione della PA, l'IA, l'IoT, la blockchain, i big data.