

Comunicazioni elettroniche sicurezza dei dati e dei sistemi

Marco Pradella
Castelfranco Veneto

Comunicazioni elettroniche sicurezza dei dati e dei sistemi

- cenno ai principali sistemi standardizzati (ISO-UNI) utilizzati a livello mondiale e nazionale, con un accenno alle future evoluzioni.
 - criteri di affidabilità, sicurezza e qualità

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- CEN ENV 12924
- fax

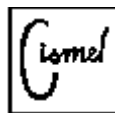


... per saperne di più ...



www.LABMEDICO.it

BITMEDICO LABSTATISTICA
LABSITI LABGOVERNO LABLIBRI



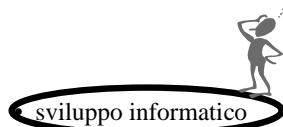
www.CISMEL.it

www.SIMEL.it



–gruppo Informatica
–gruppo Risk Management
–news: standard - linee guida

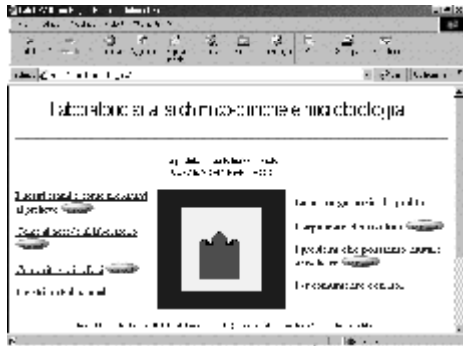
rischio e . . . sicurezza . . .



- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- CEN ENV 12924
- fax

sicurezza dei
dati e dei
sistemi

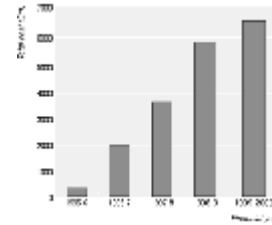
... laboratorio in internet ...



BMJ 2000;321:875-878 (7 October)

Back to basics on NHS networking

Justin Keen, fellow a, Jeremy Wyatt, reader and director, Knowledge Management Centre b, a King's Fund, 11-13 Cavendish Square, London W1M 0AN, b School of Public Policy, University College London, London WC1E 7HN



Total charges for use of NHSnet between 1995-6 and 1999-2000

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- CEN ENV 12924
- fax



Stanca

– DIRETTIVA del 18 Dicembre 2003

- **Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004.**

– (GU n. 28 del 4-2-2004)

- IL MINISTRO per l'innovazione e le tecnologie



MIT direttiva 2004 - email

- d) efficienza delle amministrazioni: posta elettronica, documento elettronico.
 - La diffusione della posta elettronica e dell'utilizzo di documenti elettronici e' presupposto indispensabile alla migliore efficienza interna. Ogni amministrazione dovrà, pertanto, dedicare rinnovato impegno a questo tema, realizzando in particolare quanto specificato nella emananda direttiva (casella di posta elettronica in dotazione a tutti i dipendenti, attivazione e utilizzo costante e tempestivo di caselle istituzionali, utilizzo interno della posta elettronica almeno in tutti i casi citati, utilizzo di posta elettronica certificata, ecc.).
 - Il progetto @P@, curato dal CNIPA, rappresenta per tutte le amministrazioni statali il punto di riferimento per ogni iniziativa, sia per quanto riguarda la partecipazione alle iniziative comuni (posta certificata, indice P.A.), sia per quanto riguarda il sostegno ai progetti specifici di ogni amministrazione.

MIT direttiva 2004 - sicurezza

- f) sicurezza delle tecnologie dell'informazione e della comunicazione.
 - Gli impegni indicati nella direttiva del marzo 2002 (autovalutazione del livello di sicurezza, adeguamento alla «base minima» di sicurezza), al momento, non sono ancora compiutamente realizzati. Le amministrazioni dovranno, pertanto, al più presto, adeguare le propria struttura, almeno, ai livelli di sicurezza minimi richiesti, rivolgendo l'attenzione sia all'ambito organizzativo che alla realizzazione di attività operative.

MIT direttiva 2005

– Direttiva del 4 gennaio 2005

• LINEE GUIDA IN MATERIA DI DIGITALIZZAZIONE DELL'AMMINISTRAZIONE

- IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

MIT direttiva 2005: abolizione carta

- ...seconda fase della digitalizzazione delle pubbliche amministrazioni, in quanto rende obbligatoria l'innovazione nella Pubblica Amministrazione nel modo più naturale: da una parte dando ai cittadini il diritto di interagire sempre, ovunque e verso qualunque amministrazione attraverso la rete; dall'altra, stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale.

MIT direttiva 2005: dematerializzazione

- I decreti legislativi concernenti il Sistema Pubblico di Connettività e Cooperazione (SPC) e il Codice dell'Amministrazione digitale forniranno l'adeguato supporto normativo in materia di dematerializzazione dei documenti, di comunicazione elettronica, di interazione a distanza, di circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove competenze professionali.

MIT direttiva 2005: ruolo dirigenti



- Per la realizzazione dei citati obiettivi e per il successo della seconda fase di digitalizzazione dell'Amministrazione, appare necessario il più ampio coinvolgimento dei dirigenti ai quali dovranno essere, conseguentemente, assegnati i precisi obiettivi da realizzare nel corso dell'anno.
- Tale coinvolgimento dovrà mirare ad ottenere, da parte della dirigenza, non soltanto il raggiungimento degli obiettivi prefissati, ma anche a suscitare un atteggiamento propositivo per la definizione dei programmi strategici delle singole Amministrazioni.
- Ogni dirigente, in vertice delle strutture in cui opera, in ciascuna amministrazione dovrà essere responsabilizzato per la definizione e per il raggiungimento di precisi obiettivi nei settori indicati dalla presente direttiva, in modo conseguente risparmio e le risorse di formazione del personale.
- Appare, infatti, indispensabile curare che, attraverso un adeguato programma di formazione tecnica, giuridica e organizzativa, sia assicurato un livello di conoscenza tale da porre la dirigenza in condizione di essere essa stessa motore del cambiamento in atto nell'agire dell'Amministrazione.

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- CEN ENV 12924
- fax



geografia della normazione

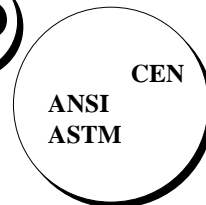
www.ANSI.org

www.ASTM.org

www.ISO.org

www.CENORM.be

www.UNI.com



CISMEL

Comitato Italiano
per la
Standardizzazione
dei Metodi
Ematologici e di
Laboratorio



www.CISMEL.it



COMMISSIONE INFORMATICA MEDICA

<http://web.uni.com/settoretecnico/ct/informaticamedica/home.shtml>

CAMPO DI ATTIVITÀ

Aspetti tecnico-informatici nel settore medico, con particolare riguardo a terminologia, modello dei dati, formato dei messaggi, strumentazione, strategie e aspetti non tecnologici, tipo etico-legali, sicurezza, riservatezza e qualità

TC CEN DI COMPETENZA TC 251 Informatica medica

TC ISO DI COMPETENZA TC 215 Informatica medica

Recenti per Informatica

- prEN 14720:2003 service request report
- prEN 12251:2003 password
- ISO/IEC 17113:2003 sviluppo messaggi
- ISO/IEC 18812:2003 interfaccia analizzatore
- ISO/DIS 17115:2005 vocabulary
- ISO/IEC 17799:2005 security
- prEN 12264:2005 strutture concetti
- prEN 1614:2005 nomenclatura laboratorio

ISO o CEN per sicurezza informatica sanitaria

- ISO/TS/ 17090-1: Health Informatics -- Public Key Infrastructure -- Part 1: Framework and overview
- ISO/TS 17090-2: Health Informatics -- Public Key Infrastructure -- Part 2: Certificate profile
- ISO/TS 17090-3: Health Informatics -- Public Key Infrastructure -- Part 3: Policy management of certification authority.
- ISO/IS ISO/22857 "Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information".
- CEN EN 12924: Medical Informatics – Security Categorisation and Protection for Healthcare Information System
- CEN prEN 12251 Health informatics - Secure user identification for health care - Management and security of authentication by passwords

ISO per sicurezza informatica sanitaria - 2

- ISO/TS 22600-1: Health informatics – privilege management and access control – Part and policy management
- ISO/TS 22600-2: Health informatics – privilege management and access control – Part models.
- ISO/TS 22600-3: Health informatics – privilege management and access control Implementations (not yet published).
- ISO/TS 21091 Health informatics –directory services for security, communications, and of professionals and patients.
- ISO technical specification 21298 Health informatics – functional and structural roles.
- ISO TR 20514, Health informatics - Electronic health record – Definition, scope and context
- ISO/IEC 27799 Health Informatics: Guideline for security management using ISO/IEC 17799

ISO per sicurezza informatica

- ISO/IEC 17799:2005, Information technology – Code of practice for information security management,
- ISO/IEC 15408, Information Technology—Security techniques—Evaluation Criteria for IT Security (Parts 1, 2 and 3), 1999.
- ISO/IEC TR 13335-1 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT security
- ISO/IEC TR 13335-2 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and Planning IT security
- ISO/IEC TR 13335-3 Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for management of IT security
- ISO/IEC TR 13335-4 Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of Safeguards
- ISO/IEC TR 13335-5 Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- **ISO/IEC 27799**
- ISO/IEC 17799
- CEN ENV 12924
- fax

ISO/IEC 27799

- **Health Informatics: Guideline for security management using ISO/IEC 17799**

– COMMITTEE DRAFT ISO/CD 27799

ISO/WD 27799

• 2005-02-11

International Electrotechnical Commission (IEC)

ISO 27999 = 17799 + sanità



sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- **ISO/IEC 17799**
- CEN ENV 12924
- fax



sicurezza in IT: profilo storico

- **USA '70: sicurezza sistemi operativi** (“*Orange book*”)
- **ISO - Europa '80: sicurezza tecnologica** (*ITSEC, ITSEM, Common criteria*)
- **UK - ISO - CEN '90: processo della sicurezza** (*BS7799, ISO/IEC 17799, ENV 16924, ...*)



ISO/IEC 17799: profilo storico

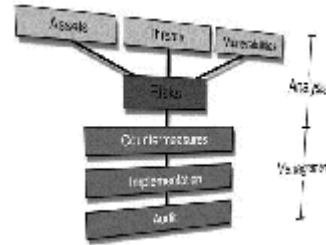
- 1990: UK DTI gruppo lavoro sicurezza informatica
- 1993: *Code of practice for information security management*
- 1995: BS7799, adottata da olanda e Svezia, respinta da ISO/IEC
- 1998: seconda parte “*Specification for information security management*”
- 1999: revisione BS7799
- 2000: adozione parte 1 come ISO/IEC 17799
- 2002: nuova versione BS7799 parte 2

ISO/IEC 17799: principi

- **garanzia Riservatezza, Integrità e Disponibilità informazione**
 - parte prima: raccomandazioni gestione sicurezza
 - 10 aree di intervento
 - 6 fasi di analisi
 - parte seconda: specifiche per la certificazione
 - 127 controlli



17799: reference to ISO/IEC 13335



ISO/IEC 17799: 10 aree intervento



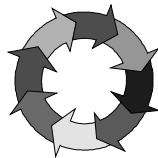
1. politica
2. principi organizzativi
3. controllo classificazione patrimonio
4. personale
5. fisica ambientale
6. comunicazioni e operazioni
7. accessi
8. sviluppo manutenzione sistemi
9. gestione continuativa
10. controlli conformità

ISO/IEC 17799: fasi sviluppo ISM

- I scopo
- II politica
- III valutazione rischio
- IV gestione rischio
- V controlli
- VI dichiarazioni applicabilità



ISO/IEC 17799: adeguamento ISO 9001:2000



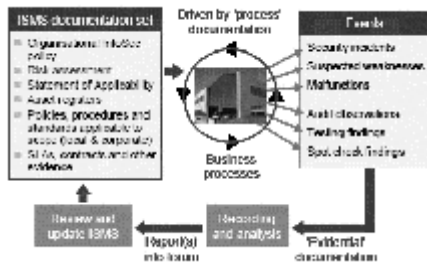
- modello Plan Do Check Act
 - pianificare
 - scopo, politica, rischio, opzioni, controlli
 - attuare
 - piano trattamento rischi, formazione, gestione operazioni e risorse, gestione incidenti
 - verificare
 - monitoraggio, audit, rischio residuo, azioni ed eventi
 - agire
 - cambiamenti, azioni correttive preventive, comunicazione risultati

Alternative Improvement Processes

Shewhart's PDCA Cycle	JCAHO's Ten-Step Process	Juran's Journey	HCA's FOCUS-PDCA Process	Joiner's Process	ODI's F-A-D-E Process
Plan	1-Responsibility 2-Scope 3-Important aspects 4-Indicators 5-Thresholds	Diagnostic phase: 1-Understand the symptom	1-Find an opportunity 2-Organize a team	1-Understand the process	1-Focus
Do	6-Exercise and monitor the system	2-Theorize the cause	3-Clarify the process	2-Eliminate errors 3-Remove the slack to simplify the process	2-Analyze the process
Check	7-Evaluate	3-Test the theory	4-Understand causes for variation	4-Reduce the variation to establish control	3-Develop a plan for improvement
Act	8-Action 9-Assess 10-Communicate	Remedial phase: 1-Establish a remedy for improvement 2-Test the remedy 3-Establish controls	5-Select the process	5-Plan for continuous improvement	4-Execute

NCCLS GP22-1999

ISO 17799 The Information Security Management System



ISO 17799 in internet

- www.iso17799-web.com/sicurezza/
- www.iso17799-web.com
- www.iso17799software.com
- www.17799.com/

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- altre norme recenti sicurezza
- CEN ENV 12924
- fax



. . . recenti per sicurezza . . .

- prEN 14484 - International transfer of personal health data
- ISO/DTR 16142 Medical devices — Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices
- CEN/TC251 NWIP “Health informatics- Assuring patient safety of health informatics products”

prEN 14484 - International transfer of personal health data - July 2003

- Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy
 - “...guidance on the High Level Security Policy which should be adopted by third country organisations involved in international informatics applications which entail transmission of person health data from an EU Member State to a non-EU Member State whose data protection is inadequate in the context of the EU Data Protection Directive [1]. Its purpose is to assist in the application of the EU Directive.... (EU Data Protection Directive)”

ISO DTR 16142 - sicurezza dispositivi

- **Medical devices — Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices**
 - Date: 2005-01-01
 - Reference number of document: **ISO/DTR 16142**
 - Committee identification: ISO/TC 210/WG 2
 - Secretariat: AAMI (for ANSI)

NWIP: safety of health informatics

- 2005-06-3
- CEN/TC 251/WG III
- **TITLE : NWIP “Health informatics- Assuring patient safety of health informatics products”**
- SOURCE : Ray Rogers (UK)

safety of health informatics

- There are many health informatics products not covered by medical devices controls. An increasing number could result in substantial adverse effects on health including death if they are not of adequate quality, examples being decision support on which there is increasing reliance, call and recall systems for screening, donor registries, electronic patient records.

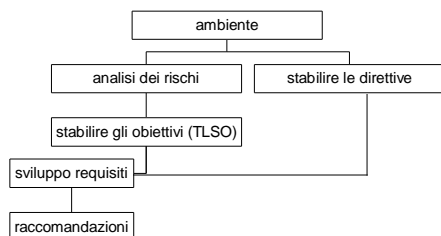
sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- altre norme recenti sicurezza
- **CEN ENV 12924**
- fax

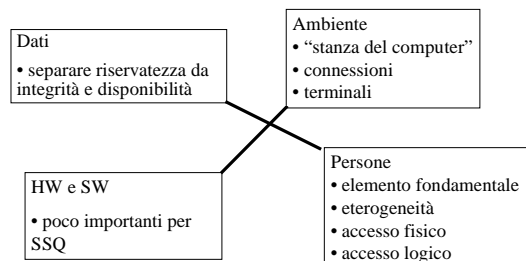
CEN/TC 251/WGIII - WGIV

ENV 12924: "Security categorisation and protection for healthcare information systems"

CEN ENV 12924: processo per garantire sicurezza



caratteristiche di un S.I. sanitario



... accesso?

BMJ 2000;321:1129-1132 (4 November)

Education and debate



Online patient-helpers and physicians working together: a new partnership for high quality health care

Based on a presentation from the Millennium Festival of Medicine

Tom Ferguson, adjunct associate professor of health informatics.

University of Texas-Houston Health Science Center, PO Box 20036, Houston, TX



ENV 12924: Processo di classificazione della sicurezza e specificazione dei requisiti

- Passo 1. Valutare ACI (disponibilità - riservatezza - integrità)
- Passo 2. Individuare la categoria
- Passo 3. Individuare i requisiti di base
- Passo 4. Costruire il profilo di protezione: categoria + requisiti di base + requisiti di livello superiore
- Passo 5. Realizzazione dei requisiti
- Passo 6. Procedere con la sicurezza



A = disponibilità

- domanda 1: la non disponibilità delle informazioni può causare cattivo o prolungato trattamento ?
- domanda 2: se le informazioni non sono disponibili, ne risultano conseguenze finanziarie, legali o altro ?

considerare lo scenario peggiore - non tener conto di copie elettroniche o su carta

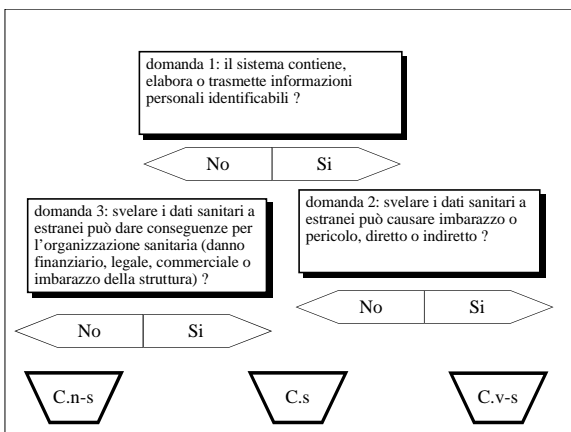
non critica
 <<
 critica
 A.n-c
 >>
 A.c

C = riservatezza (confidentiality)

- domanda 1: il sistema contiene, elabora o trasmette informazioni personali identificabili ?
- domanda 2: svelare i dati sanitari a estranei può causare imbarazzo o pericolo, diretto o indiretto ?
- domanda 3: svelare i dati sanitari a estranei può dare conseguenze per l'organizzazione sanitaria (danno finanziario, legale, commerciale o imbarazzo della struttura) ?

considerare attentamente i dati anche non identificati direttamente, ma identificabili mediante inferenza
 considerare lo scenario peggiore - non tener conto dei rimedi esistenti

non sensibile
 <<
 sensibile
 <<
 molto sensibile
 C.n-s
 <<
 C.s
 <<
 C.v-s



I = integrità

- domanda 1: errori o mancanze possono causare cattivo o prolungato trattamento ?
- domanda 2: in caso di errori o mancanze, risultano conseguenze finanziarie, legali o altro ?

considerare lo scenario peggiore - non tener conto di eventuali misure correttive

non critica
 <<
 critica
 I.n-c
 <<
 I.c

categorie

- I: A.nc, Cs, L.n-c
- II: A.nc, Cs, L.c
- III: A.c, Cs, L.c
- IV: A.nc, C.v-s, L.n-c
- V: A.nc, C.v-s, L.c
- VI: A.c, C.v-s, L.c

ENV 12924: ambiente fisico

Accesso fisico	Lontananza		PEA
N	S		1
N	N		2
	staff presente a pubblico presente	sorvegliato a pubblico assente	
S	S	S	3
S	S	N	4
S	N	N	5
S	N	S	6

ENV 12924: connessione fisica

Rete		PCA
N		1
	permanente	
S	N	2
S	S	3

ENV 12924: connessione logica

Un solo dominio		LCA
N		1
	una sola struttura sanitaria	
S	N	2
S	S	3

Profilo di protezione I Categoria I: A.nc, Cs, L.n-c

- sistema
 - pw (+hw PEA 5-6)
 - preced. log-on
 - autom. log-out
 - privilegi
 - registrazioni etc..
- requisiti amministrativi
 - security manager
 - security policy
 - virus
 - manutenzione
 - documentazione
- requisiti personale
 - assunzione
 - gestione
 - addestramento
 - fine rapporto
- requisiti fisici e ambientali
 - computer principale
 - furto
 - elettricità, aria, fuoco, acqua

requisiti aggiuntivi Profili di protezione II-VI

- sistema
 - identificazione terminali
 - registrazione operazioni
 - backup affidabile
 - firewalls
 - etc..
- requisiti amministrativi
 - quality plan
 - prove sistema separato
 - verifiche documentate
 - etc..
- requisiti personale
 - idem
- requisiti fisici e ambientali
 - accesso controllato
 - identificazione
 - orari
 - area esterna, parcheggio etc..

requisiti specifici Profili di protezione II-VI

- profilo II
 -
 -
 -
- profilo III
 -
 -
 -
 -
- profilo IV
 -
 -
 -
- profilo V
 -
- profilo VI
 -
 -

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- altre norme recenti sicurezza
- CEN ENV 12924
- fax

attenti al fax

- Printed copies after fax report
Medical Laboratory Observer, March, 2005 by Daniel M. Baer

Q Our laboratory follows up every faxed lab report with a printed hard copy. Some doctors, however, do not like receiving multiple copies of the same report. Are your experts aware of any requirements for sending printed copies in addition to faxed reports?

A I am not aware of any requirement for sending a printed hard copy of a report after sending a fax report. There are several things you should keep in mind about faxed reports, however.

First, the fax machine must be secure; in order to comply with HIPAA requirements, only persons authorized to see patients' confidential medical information should have access to faxed reports. Second, your laboratory should have a method for confirming that faxed reports are received. Most fax machines have the ability to send error messages if the fax is not received correctly. Finally, the lab should have a procedure for investigating any reports of faxes that were not received.

--Daniel M. Baer, MD
Professor Emeritus
Department of Pathology
Oregon Health and Science University
Portland, OR

sicurezza dei dati e dei sistemi

- sviluppo informatico
- direttive informatiche PA
- standard informatici
- ISO/IEC 27799
- ISO/IEC 17799
- altre norme recenti sicurezza
- CEN ENV 12924
- fax

... per saperne di più ...



www.LABMEDICO.it

BITMEDICO LABSTATISTICA
LABSITI LABGOVERNO LABLIBRI



www.CISMEL.it

www.SIMEL.it



-gruppo Informatica
-gruppo Risk Management
-news: standard - linee guida

www.tecnidilaboratorio.it