Formez PA

PRIVACY IN RETE

Cosa dicono le norme?

Avv. Prof. Ernesto Belisario

www.ernestobelisario.eu

SLB

BELISARIO

STUDIO LEGALE

Internet, 28 marzo 2012

BIBLIOGRAFIA

1) **Giuseppe Cassano – Carmelo Giurdanella**, *Il Codice della Pubblica Amministrazione Digitale*. Giuffrè – 2005.

2) **Angelo Giuseppe Orofino**, *Forme elettroniche e procedimenti amministrativi, Cacucci – 2008.*

3) **Marianna Quaranta**, *Il Codice della Pubblica Amministrazione Digitale*. Liguori – 2007.

4) **Ernesto Belisario**, *La nuova Pubblica Amministrazione Digitale*, Maggioli – 2009.

5) **Gilberto Marzano**, *Conservare il digitale*, Editrice Bibliografica - 2011

5) **Pierluigi Ridolfi**, *Il Nuovo Codice della Amministrazione Digitale*, SIAV - 2011

6) **AA. VV.**, *Il nuovo CAD: manuale d'uso*, ForumPA Edizioni, 2011

SITOGRAFIA

1) **Ministero per la Pubblica Amministrazione e l'Innovazione**
   www.innovazionepa.gov.it

2) **Dossier "Codice Amministrazione Digitale"**
   www.governo.it/GovernoInforma/Dossier/codice_amministrazione_digitale/

3) **Senato della Repubblica - Centro Studi**
   www.senato.it/documenti/repository/dossier/studi/2010/Dossier_251.pdf

4) **DigitPA**
   www.digitpa.gov.it

5) **Egov**
   www.egov.maggioli.it

6) **Diritto 2.0**
   blog.ernestobelisario.eu

7) **Dgit@Lex**
   www.digita-lex.it/

SOMMARIO

- Introduzione al concetto di privacy
- La sicurezza informatica
- I siti Web delle PA
- Privacy e trasparenza

Formez PA

LA PRIVACY

PRIVACY

Diritto di essere lasciati tranquilli

Tutela della riservatezza

PRIVACY

- Diritto ad essere lasciato solo (1890 Warren e Brandeis)

↓

- Diritto a chiedere di se stesso
- Diritto di scegliere quel che si è disposti a rivelare agli altri
- Diritto di controllare l'uso delle informazioni che ci riguardano

PRIVACY

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla *tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

in ITA legge 31 dicembre 1996, n. 675 (c.d. "legge privacy")

Diritto a:

non fare circolare i propri dati personali;

controllarne l'utilizzazione;

far cessare il trattamento illecito.

PRIVACY

art. 1. primo comma Direttiva 95/46/CE “Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle *persone fisiche* e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali”

art. 1. primo comma legge del 31 dicembre 1996 n. 675 “La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle *persone fisiche*, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle *persone giuridiche* e di ogni altro ente o associazione”

PRIVACY

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al *trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.*

Decreto legislativo 30 giugno 2003, n. 196 -
Codice in materia di protezione dei dati personali

CODICE PRIVACY

Parte generale — Art. 1 – 45 — Tutti i trattamenti

Parte speciale

Ambito giudiziario	art. 46 – 52
Forze di polizia	art. 53 – 57
Difesa e sicurezza dello stato	art. 58
Ambito pubblico	art. 59 – 74
Ambito sanitario	art. 75 – 96
Scopi storici, statistici, scientifici	art. 97 – 110
Lavoro e Previdenza Sociale	**art. 111 – 116**
Bancario, finanziario e assicurativo	art. 117 – 120
Comunicazioni elettroniche	**art. 121 – 133**
Videosorveglianza	**art. 134**
Giornalismo	art. 136–139

AMBITO DI APPLICAZIONE

- **QUALI MISURE ?**
- **CHI E' TENUTO AD ADOTTARLE ?**

Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque e' stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
(art. 5, comma 1, d. lgs. n. 196/2003)

fini esclusivamente personali

Definizioni

A CHI SI APPLICA?

CHIUNQUE E' STABILITO NELLO STATO → anche " dati all'estero"

NON SI APPLICA

PERSONE FISICHE

- Fini esclusivamente personali
- No comunicazione sistematica
- No diffusione

Definizioni

TRATTAMENTO (art. 4 lett. a)

Anche se non sono contenuti in una banca dati

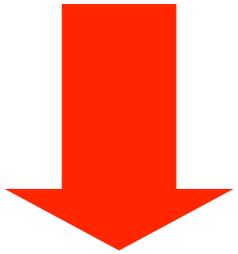
- Raccolta
- Registrazione
- Organizzazione
- Conservazione
- Consultazione
- Elaborazione
- Modificazione
- Selezione
- Estrazione
- Raffronto
- Utilizzo
- Interconnessione
- Blocco
- **Comunicazione**
- **Diffusione**
- Cancellazione
- Distruzione

COMUNICAZIONE → A persone determinate

DIFFUSIONE → A persone indeterminate

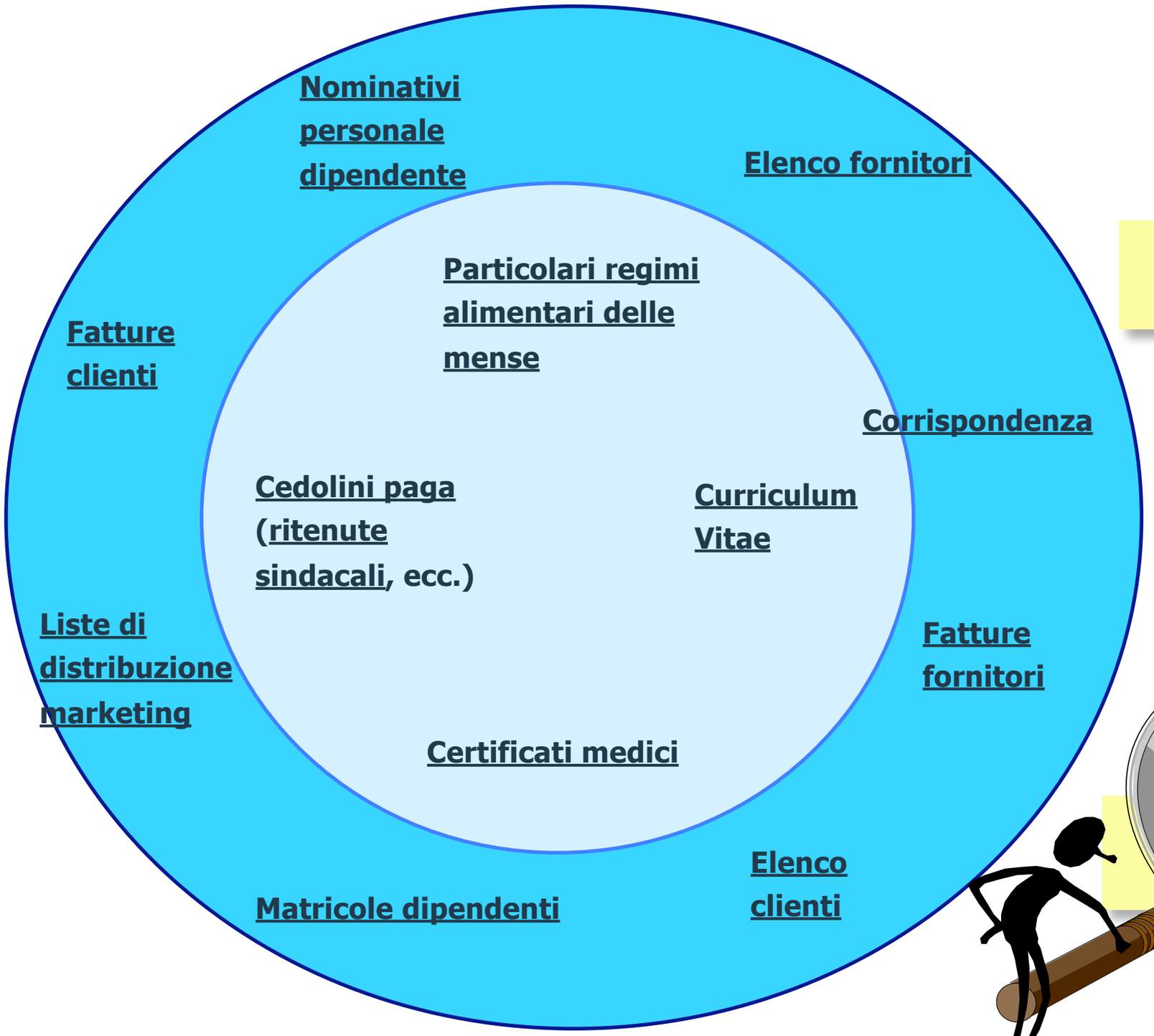
DEFINIZIONI

- **Dato personale**: qualunque informazione relativa a persona fisica, giuridica, ente o associazione identificate o identificabili

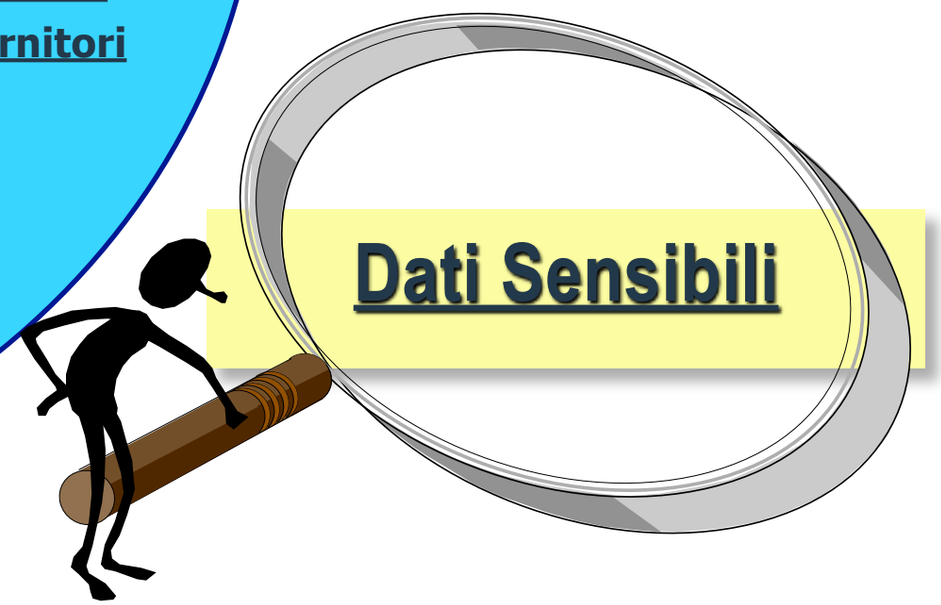


- Codice fiscale
- Recapiti
- Lavoro
- Attività economiche
- Istruzione

QUADRO RIEPILOGATIVO



Dati Personali



ENTI PUBBLICI

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

ADEMPIMENTI BASE

- *DESIGNAZIONI*
- *INFORMATIVA*
- **CONSENSO**
- *NOTIFICAZIONE*
- *MISURE DI SICUREZZA*

ORGANIZZAZIONE DELLA PRIVACY

IL TITOLARE DEL TRATTAMENTO DEVE INDIVIDUARE FORMALMENTE, CON ATTO SCRITTO, I SOGGETTI CHE HANNO TITOLO A TRATTARE I DATI

LE DESIGNAZIONI

- *responsabili del trattamento (interni ed esterni):* questa figura, la cui designazione è facoltativa, ricorre frequentemente in presenza di articolazioni interne delle realtà produttive ovvero in presenza di servizi in outsourcing (es. gestione buste paga)
- *incaricati:* questa figura, la cui designazione è obbligatoria, individua le persone fisiche che - materialmente - compiono operazioni di trattamento dati all'interno dell'azienda

LA SICUREZZA INFORMATICA

"Complesso di tutte le operazioni e accorgimenti adottati al fine di rendere vani i tentativi di attacchi (passivi ed attivi) che possono essere perpetrati ai danni di un sistema informatico ".

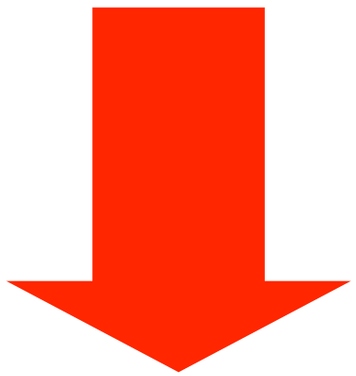
LA SICUREZZA INFORMATICA

SICUREZZA DEI DATI E DELLE INFORMAZIONI

Confidenzialità

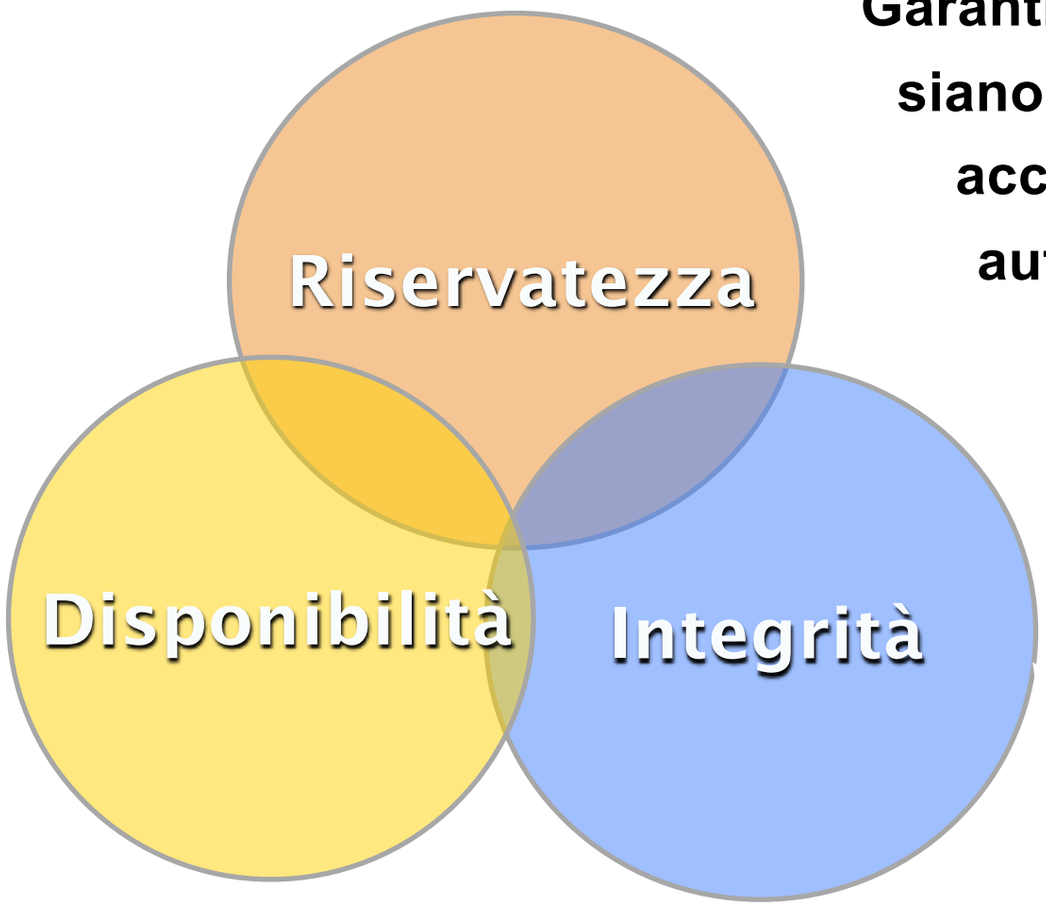
Integrità

Disponibilità



- ☐ Legge di Ranum (il software non basta)
- ☐ La sicurezza informatica totale non esiste

SICUREZZA DEI DATI E DEI SISTEMI



Garantire che i dati siano protetti da accessi non autorizzati

Garantire che i dati siano disponibili agli utenti autorizzati

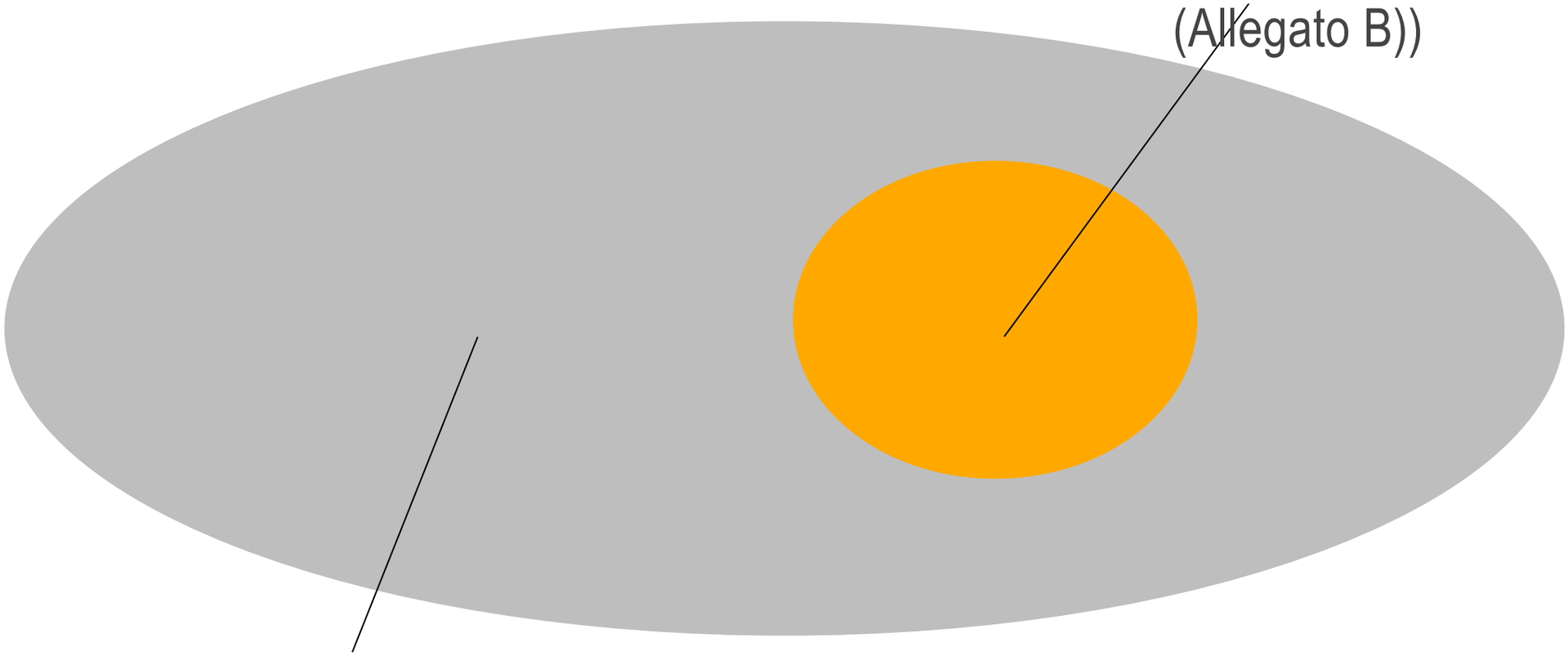
Garantire che i dati siano aggiornati ed integri

MISURE DI SICUREZZA

il D. Lgs. n. 196/2003 prevede due distinti tipi di misure di sicurezza

- ***misure minime (All. B)***: il mancato rispetto costituisce reato
- ***misure idonee (art. 31)***: la mancata adozione di esse espone al risarcimento dei danni

SICUREZZA DEI DATI E DEI SISTEMI



IDONEE

(art. 31, 1)

OBBLIGHI DI SICUREZZA

Art. 31 D. Lgs. n. 196/2003

In relazione a:

- conoscenze acquisite dal progresso tecnico
- natura dei dati
- specifiche caratteristiche del trattamento

IDONEE E PREVENTIVE MISURE DI SICUREZZA

riducono al minimo

rischi di:

- distruzione/perdita di dati
- accesso non autorizzato
- trattamento non consentito/non conforme

MISURE MINIME DI SICUREZA

Art. 33 D. Lgs. n. 196/2003

Obblighi di sicurezza (art. 31)

↓

MISURE MINIME

↓

Livello minimo di protezione dei dati

ALLEGATO B

1-26 Trattamenti **con** strumenti elettronici

27-29 Trattamenti **senza** strumenti elettronici

Strumenti elettronici **>** elaboratore

MISURE MINIME

Trattamento con strumenti elettronici

Autenticazione (1-11) - parola chiave

- rilevazione biometrica

Autorizzazione (12-14)

Altre misure (15-18) - antivirus

- patch, upgrade

- back up

Documento programmatico sulla sicurezza (19)

Dati sensibili o giudiziari (20-24)

Misure di tutela e garanzia (25-26)

STRUMENTI ELETTRONICI

Riguardo agli ELABORATORI

- credenziali di **autenticazione informatica** (user-id e password)
- sistema di **autorizzazione** (singole operazioni)
- misure di **protezione** e **ripristino** dati (antivirus; firewall; back-up)

AUTENTICAZIONE INFORMATICA

La ***password*** (o altro dispositivo di autenticazione che può essere anche una caratteristica biometrica) deve essere conosciuta esclusivamente dall'incaricato, restare in suo esclusivo possesso ed essere modificata almeno ogni 6 mesi, o ogni 3 mesi se i dati trattati sono sensibili o giudiziari.

Anche il codice di identificazione è unico e una volta assegnato ad un incaricato non può essere assegnato ad altri.

Codice di identificazione e password sono disattivate se non sono utilizzate da almeno 6 mesi o in caso di perdita della qualità che consente all'incaricato di accedere ai dati.

Agli incaricati vengono impartite indicazioni sul trattamento ed è prescritto di adottare le cautele necessarie per assicurare la segretezza della password e dei dispositivi di accesso, nonché di non lasciare incustodito ed accessibile a terzi lo strumento elettronico durante il trattamento.

PAROLA CHIAVE

Fattori di sicurezza

lunghezza (8 caratteri)

composizione, scelta e digitazione (non ha riferimenti all’incaricato)

distribuzione e modifica (modificata al 1° utilizzo)

vita utile (6 mesi/3 mesi)

titolarità (individuale)

FIREWALL

Dispositivo che inserisce una barriera che blocca ogni accesso non autorizzato tra la propria Azienda e la rete Internet (hacker, virus, spyware, ecc.).

AGGIORNAMENTO

- **Annuale** per dati comuni
- **Semestrale** per dati sensibili

BACK UP

PREVENZIONE

DISTRUZIONE O PERDITA DATI

Back - up automatizzati
giornalieri o massimo settimanali

RECUPERO

IN CASO DI DANNEGGIAMENTO

ANTIVIRUS

I dati personali devono essere protetti **contro il rischio di intrusione e dall'azione dei programmi di cui all'art. 615-quinquies** c.p. mediante l'attivazione di idonei strumenti elettronici da aggiornare almeno ogni 6 mesi.

Controllo mediante computer non collegato alla rete dei floppy-disk provenienti dall'esterno.

Interazione solo con sistemi dotati di programmi antivirus

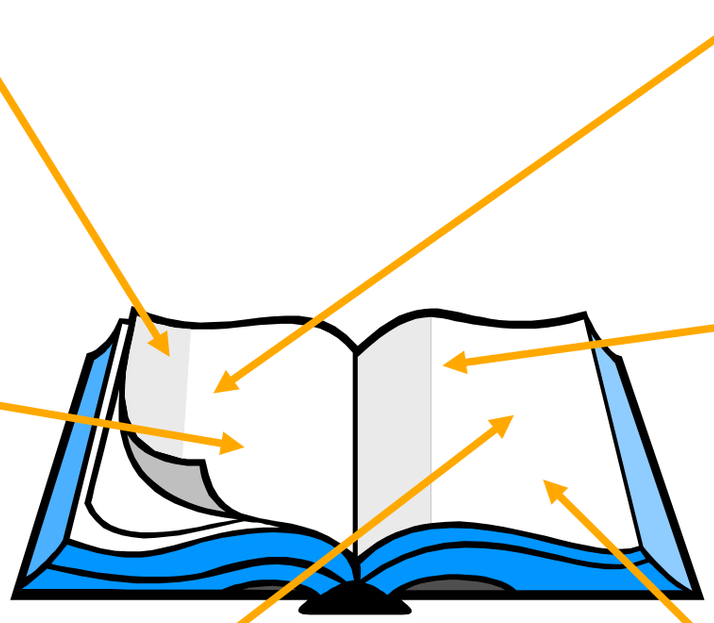
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Analisi dei rischi

Compiti e responsabilità

Criteri e procedure per l'integrità dei dati

Criteri tecnici ed organizzativi per la protezione dei locali



Criteri e procedure per la sicurezza delle trasmissioni

Piano di formazione per gli incaricati

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Entro il 31 marzo di ogni anno:

elenco dei trattamenti

distribuzione dei compiti

analisi dei rischi

misure da adottare

ripristino dei dati

interventi formativi

SANZIONI PENALI

Art. 169 (Misure di sicurezza) 1° comma

Mancata adozione delle misure MINIME (art.33)

arresto fino a 2 anni o

ammenda da 10 a 50 mila euro

SANZIONI PENALI

Art. 169 (Misure di sicurezza) 2° comma

Termine per regolarizzarsi (> 6 mesi)

adempimento e

pagamento di 12.500 euro

estinzione del reato

SANZIONI CIVILI

Risarcimento del danno

Mancata adozione delle misure IDONEE (art.31)

Art.15: il danno è risarcito ai sensi dell'art. 2050 c.c.

(se non prova di aver adottato tutte

le misure idonee a evitarlo)

+

danno non patrimoniale


Chelmsford (A 414)
Chipping Ongar A 128
Brentwood
Kelvedon Hatch A 128
Industrial Estates
Secret Nuclear Bunker

SISTEMI INFORMATIVI PUBBLICI

Adeguamento tecnologico ed organizzativo

- Piena attuazione normativa protocollo informatico e gestione automatizzata dei procedimenti (*Dpr n. 445/2000*; *Dpcm 31 ottobre 2000*)
- Sicurezza dei dati e dei sistemi (*art. 51*)

> *"1. Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71, garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.*
>
> *2. I documenti informatici delle Pubbliche Amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta."*

E’ IMPORTANTE

Art. 20 CAD

1-bis. L'idoneita' del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualita', sicurezza, integrita' ed immodificabilita', fermo restando quanto disposto dall'articolo 21

Art. 21 CAD

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità , sicurezza, integrità e immodificabilita

SISTEMI INFORMATIVI PUBBLICI

La diffusione delle tecnologie informatiche nelle PA e la tenuta di archivi informatizzati rende necessario:

- Individuare procedure per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture

- Garantire la continuità del servizio anche quando erogato mediante tecnologie ICT (art. 50 bis)

- Individuare le procedure da mettere in atto in situazioni di emergenza, che devono riguardare le risorse umane, le risorse strumentali, le strutture e le infrastrutture

DEFINIZIONE DI CONTINUITÀ OPERATIVA E DI DISASTER RECOVERY

Dalle "Linee guida per la continuità operativa della Pubblica Amministrazione" (Quaderno n. 28 DigitPA):

- *Continuità operativa: insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.*

- *Disaster Recovery: insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.*

NORME IN MATERIA DI CONTINUITÀ OPERATIVA

- Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)

- Decreto legislativo 30 dicembre 2010, n. 235 (Gazz. Uff. 10 gennaio 2011, n. 6):

  Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

NORMATIVA PRIVACY

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

(Art. 31, D. Lgs. n. 196/2003)

NUOVO CAD

1.In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono :

il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.".

DEFINIZIONE

Disastro: Una calamità improvvisa e non pianificata che causa gravi danni o perdite.

QUALCHE ESEMPIO...

- Calamità naturali (es. terremoti)
- Problemi nell'alimentazione elettrica
- Guasti della rete
- Eventi fortuiti (es. incendi)
- Inagibilità dei locali
- Malfunzionamenti del sistema informatico
- ... combinazione di due o più degli eventi sopra descritti.

CONTENUTI DEL PIANO

- ☑ Scopo e campo di applicazione, dove si identificano gli elementi fisici (quali le sedi, le aree all'interno delle sedi, il data center, ecc.) e funzionali (le attività di business o i servizi) dell'organizzazione coperti dal piano

- ☑ Obiettivi di continuità degli elementi coperti dal piano

- ☑ Ruoli e responsabilità nella gestione dell'emergenza, con particolare evidenza dei ruoli decisionali di vertice dell'organizzazione;

- ☑ Criteri di attivazione delle procedure di emergenza (le condizioni che determinano la dichiarazione di disastro)

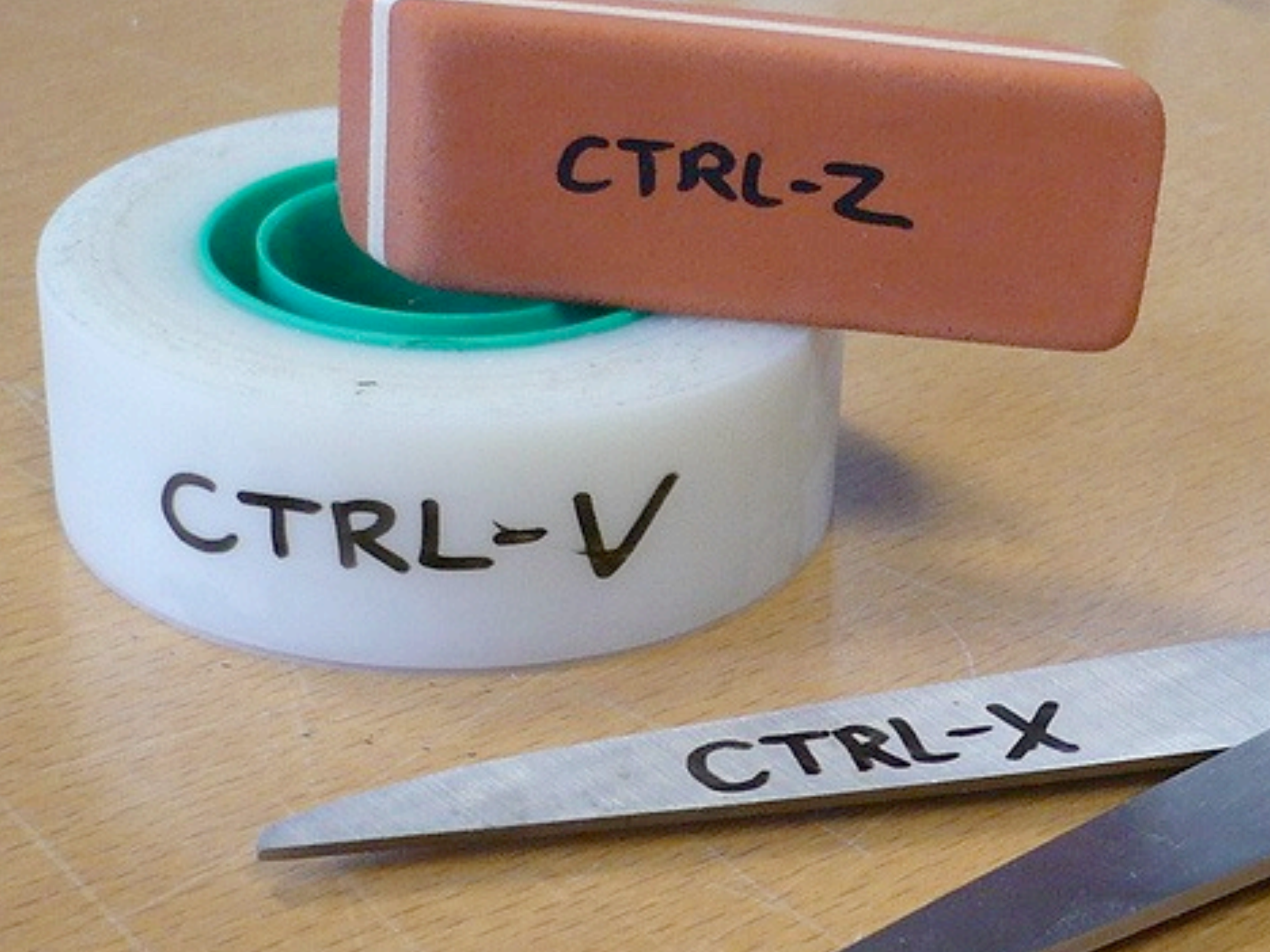
- ☑ Procedure di attuazione in risposta alla condizione di di emergenza (la reperibilità del personale chiave, le modalità di comunicazione ai dipendenti, le modalità di comunicazione agli esterni interessati –nel caso di PA: cittadini, imprese, altre PA-, il piano di disaster recovery);

- ☑ Flusso di informazioni e processi di documentazione

- ☑ Modalità di verifica e di aggiornamento del Piano

Formez PA

I SITI WEB DELLE PA


CTRL-Z
CTRL-V
CTRL-X

LE LINEE GUIDA

Ogni sito pubblico deve fornire ai propri utenti una informativa chiara e completa in merito a:

- caratteristiche generali dei contenuti proposti dal sito e loro corretto utilizzo;

- modalità di trattamento dei dati eventualmente resi disponibili dagli utenti.

LE LINEE GUIDA

La consultazione della *policy* deve essere costantemente disponibile all'interno del piè di pagina del sito. È opportuno distinguere i due tipi di contenuti:

1) il primo sarà indirizzato dall'etichetta "Note" o "Note legali";

2) il secondo dall'etichetta "Privacy" o "Protezione dei dati personali".

NOTE LEGALI

Nelle “Note legali” devono essere fornite informazioni almeno in relazione ai seguenti argomenti:

a) copyright: possibilità e limitazioni in ordine all’utilizzo dei contenuti del sito;

b) utilizzo del sito: responsabilità derivanti dall’utilizzo del sito;

c) accesso a siti esterni collegati: responsabilità sui contenuti di siti esterni collegati;

d) download: regole per l’utilizzo dei materiali scaricabili dal sito.

PRIVACY

Nella sezione “Privacy” devono essere descritte le modalità di gestione del sito in riferimento al trattamento dei dati personali e degli utenti che interagiscono con i servizi resi disponibili. Si tratta di una informativa da rendere ai sensi del Decreto legislativo 2003, n. 196 “Codice in materia di protezione dei dati personali”.

PRIVACY

In particolare, devono essere oggetto di attenzione gli adempimenti “informativi”, con cui - cioé - si dica all’utente cosa si farà dei suoi dati personali, a chi li si comunicherà, quali sono i suoi diritti e a chi rivolgersi per eventuali lamentele.

CONTENUTO INFORM

- *Dati di navigazione*
- *Dati forniti volontariamente dall'utente*
- *Cookies*

TIPI DI DATI TRATTATI

Dati di navigazione

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo ed all'ambiente informatico dell'utente. Tali dati devono essere utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e sono cancellati immediatamente dopo l'elaborazione. I dati possono essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito.

TIPI DI DATI TRATTATI

Dati forniti volontariamente dall'utente

Molti servizi web prevedono l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati sul sito che comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. Specifiche informative di sintesi (disclaimer) debbono essere visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta. Deve essere inoltre indicato il trattamento di dati sensibili o giudiziari eventualmente forniti dall'utente nel corpo della mail.

PRIVACY

Cookies

Nessun dato personale degli utenti deve essere di proposito acquisito dal sito. Non deve essere fatto uso di cookies per la trasmissione di informazioni di carattere personale, né debbono essere utilizzati cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti. L'uso di cookies di sessione (che non debbono venire memorizzati in modo persistente sul computer dell'utente e debbono svanire con la chiusura del browser) deve essere strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito, evitando il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti, e non debbono consentire l'acquisizione di dati personali identificativi dell'utente. L'utilizzo di cookies permanenti deve essere strettamente limitato all'acquisizione di dati statistici relativi all'accesso al sito. L'eventuale disabilitazione dei cookies sulla postazione utente non deve influenzare in alcun modo l'interazione con il sito.

TRASPARENZA E PRIVACY: RELAZIONE COMPLICATA

Formez PA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERAZIONE 19 aprile 2007.

Linee guida in materia di trattamento di dati personali per finalità di pubblicazioni e diffusione di atti e documenti di enti locali.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LE NUOVE REGOLE

Fermo restando che soggetti pubblici possono utilizzare informazioni personali per lo svolgimento delle proprie funzioni istituzionali anche in mancanza di una norma di legge o di regolamento che preveda espressamente il trattamento di dati personali senza richiedere il consenso dell'interessato, a seconda del fine perseguito, le pubbliche amministrazioni dovranno valutare, di volta in volta, l'effettiva necessità di diffusione di tali dati, nonché utilizzare strumenti e accorgimenti tecnici diversi al fine assicurare forme corrette e proporzionate di conoscibilità di tali informazioni

LE NUOVE REGOLE

- impedendo la loro indiscriminata e incondizionata reperibilità in Internet. A questo scopo bisogna valutare se tali dati debbano essere o meno reperibili mediante motore di ricerca esterno o interno allo stesso sito;
- garantendo il rispetto dei principi di qualità ed esattezza dei dati. A tale scopo le PA dovranno adottare idonee misure per eliminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni delle informazioni e dei documenti resi disponibili tramite internet, come , ad esempio, l'inserimento dei "dati di contesto" (es. data di aggiornamento, periodo di validità, amministrazione) all'interno del contenuto informativo dei documenti, e l'indicazione delle fonti attendibili per il reperimento dei medesimi documenti;

LE NUOVE REGOLE

- delimitando la durata della loro disponibilità on line. Nel caso in cui la disciplina di settore stabilisca un limite temporale alla pubblicazione degli atti , le PA dovranno assicurarsi che tale limite temporale venga rispettato, al contrario, nel caso in cui tale limite non sia stabilito a priori, sarà cura delle PA stabilire tale limite in relazione alle esigenze di volta in volta perseguite;

LE NUOVE REGOLE

- evitando la duplicazione massiva dei file contenenti dati personali. Al fine di ridurre il rischio di riproduzione massiva di tali file mediante software e programmi automatici e il riutilizzo dei contenuti informativi in ambiti e contesti differenti, le PA dovranno far ricorso ad appositi accorgimenti come ad esempio, l'utilizzo di di firewall di rete in grado di riconoscere accessi che risultino anomali per numero rapportato all'intervallo di tempo di riferimento oppure di opportuni filtri applicativi che, a fronte delle citate anomalie, siano in grado di rallentare l'attività dell'utente e di mettere in atto adeguate contromisure.

LE NUOVE REGOLE

Le Amministrazioni dovranno valutare gli interessi coinvolti sempre in riferimento al singolo caso, individuando, di volta in volta, le necessarie cautele per bilanciare tali interessi in base ai principi indicati dall'articolo 11 del D.Lgs 196/2003 (Codice in materia di protezione dei dati personali), ed in particolare quelli di:

- necessità (individuare l'obbligo o meno di pubblicità legale);
- proporzionalità (pertinenza e non eccedenza);
- diritto all'oblio del soggetto interessato coinvolto attraverso tecniche informatiche che escludano l'indicizzazione da parte dei motori di ricerca.

SANZIONI E RESPONSABILITA’

GIVE US SOME FEEDBACK

GRAZIE

SLB

BELISARIO

STUDIO LEGALE

www.ernestobelisario.eu

facebook.com/amministrazionedigitale

edu@ernestobelisario.eu

ernesto.belisario@pec.studiobelisario.it