Progetto GIT

La privacy e la gestione del sistema informativo comunale

(a cura del progetto GIT)

Luglio 2010

IL PROCESSO PRIVACY

- Principi generali
- Soggetti
- Diritti dell'interessato
- I soggetti pubblici
- Misure di sicurezza

IL NUOVO CODICE PRIVACY

Il 29 luglio 2003

è stato pubblicato sulla Gazzetta Ufficiale

il nuovo Codice in materia di

protezione dei dati personali

(G.U. Serie generale n. 174,

Supplemento ordinario n. 123/L)

EVOLUZIONE NORMATIVA

- **direttiva 95/46/CE del 24.10.1995**
  Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati

- **direttiva 2002/58/CE del 12.07.2002**
  Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche

EVOLUZIONE NORMATIVA

- **Legge n. 675 del 31 dicembre 1996**
  Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

- **DPR 28 luglio 1999 n. 318**
  Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675

- **Legge 3 novembre 2000 n. 325**
  Disposizioni inerenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31 dicembre 1996, n. 675

PRINCIPI GENERALI

Oggetto e ambito di applicazione

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.
Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale.

Il "Codice Privacy" disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

PRINCIPI GENERALI

Oggetto e ambito di applicazione

Chiunque ha diritto alla protezione dei dati personali che lo riguardano

il diritto alla protezione dei dati personali, quale prerogativa fondamentale della persona, è stato introdotto nell'ordinamento in attuazione dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea del 7.12.2000 e deve considerarsi quale **diritto autonomo e distinto** rispetto al diritto alla riservatezza sostanziandosi nel diritto del suo titolare di conoscere e controllare la circolazione delle informazioni che lo riguardano.

PRINCIPI GENERALI

Oggetto e ambito di applicazione

Chiunque ha diritto alla protezione dei dati personali che lo riguardano

- diritto all'identità personale
- diritto alla riservatezza
- diritto alla protezione dei dati personali

.

PRINCIPI GENERALI

- **art.1**
  diritto alla protezione dei dati personali

- **art.2**
  semplificazione nell'alta tutela dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, riservatezza, identità personale e diritto alla protezione dei dati personali

PRINCIPI GENERALI

- **art. 3**
  principio di necessità

- **art. 11**
  principi di:
  - finalità
  - liceità
  - proporzionalità: pertinenza e non eccedenza
  - correttezza e completezza

PRINCIPI GENERALI

Art. 11 Modalità del trattamento e requisiti dei dati

I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

PRINCIPI GENERALI

- In applicazione dell'art. 11 i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi

- I dati che risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene

- Pubblicazioni internet: il titolare, una volta perseguite le finalità poste alla base del trattamento, deve garantire il rispetto del Diritto all'oblio dell'interessato

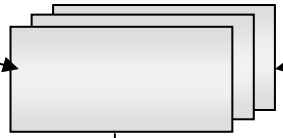
PRINCIPI GENERALI

- La cancellazione di dati (su richiesta dell'interessato o in occasione della cessazione del trattamento) = distruzione dei documenti => deve essere autorizzata dalla Soprintendenza archivistica (art. 22 c. 5 D. Lgs. 196/2003 e art. 21 c. 1-d D. Lgs. 42/2004)

- L'aggiornamento, la rettifica o l'integrazione di dati viene fatta assicurando la distinzione tra fonte originaria (che si continua a conservare) e documentazione successivamente acquisita (art. 7 c. 1 alleg. al Provvedimento 14 mar. 2001 n. 8/P/2001 del Garante)

CONTESTO ORGANIZZATIVO-

Gestione delle informazioni



Sistemi informativi

- Definizione delle **logiche organizzative** (tempi, ruoli, responsabilità) per la gestione delle informazioni cartacee

- Definizione delle **logiche organizzative** (tempi, ruoli, responsabilità) per la gestione delle informazioni elettroniche

Organizzazione

Trasparenza | **Efficienza** | **Efficacia**

Rispetto della privacy

Obiettivo Finale

Ottimizzare il rapporto con l'utenza

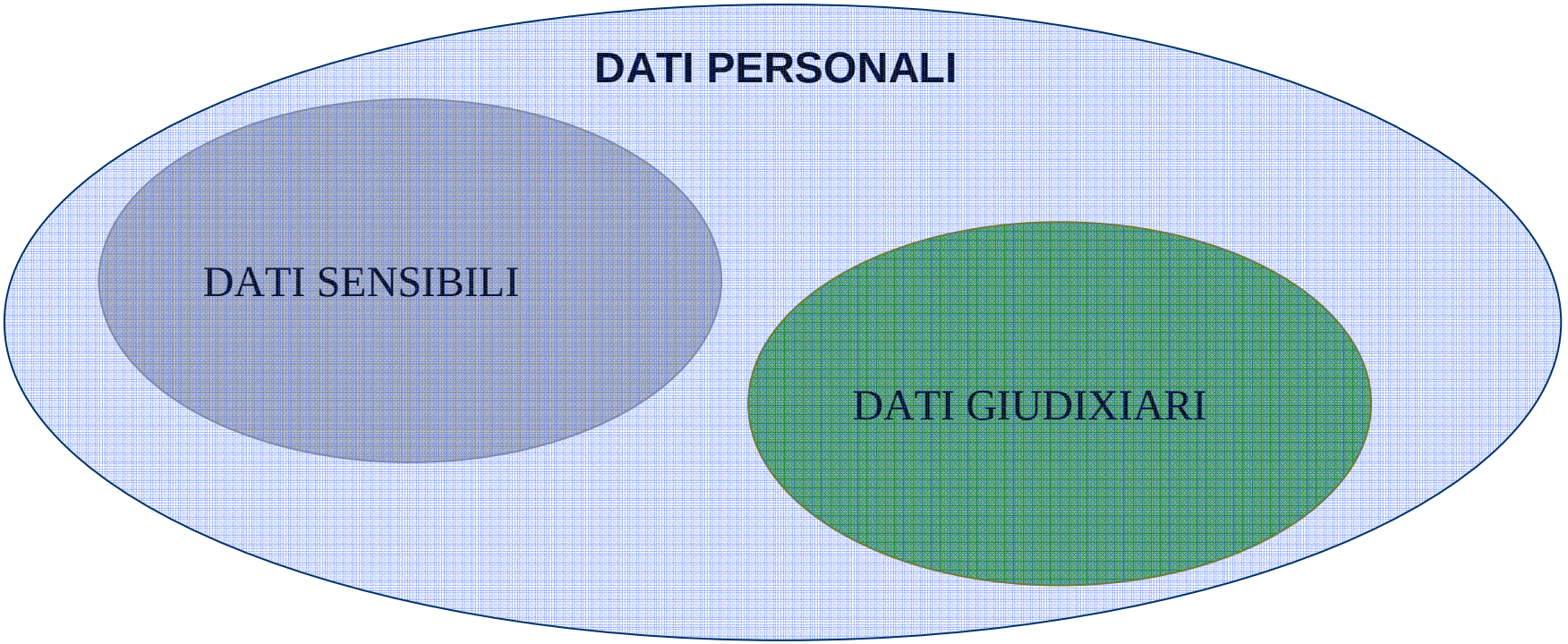
DEFINIZIONI

Art. 4 Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Esempio: nome e cognome o denominazione; indirizzo o sede; codice fiscale; ma anche una foto, la registrazione della voce di una persona, la sua impronta digitale o vocale.

DEFINIZIONI



DEFINIZIONI

Art. 4 Dato sensibile

Quei particolari dati personali idonei a rivelare:

origine: razziale ed etnica	anagrafe
convinzioni: religiose, filosofiche o di altro genere	servizi alla persona, cultura, educazione, commercio,
opinioni: politiche, adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	anagrafe, personale, servizi alla persona, cultura, polizia locale, commercio,
stato di salute e **vita sessuale**	polizia locale, personale, servizi alla persona, educazione

DEFINIZIONI

Art. 4 Dato giudiziario

Quei particolari dati personali idonei a rivelare:

provvedimenti relativi a: condanne penali, procedimenti penali in corso, sanzioni amministrative derivanti da reati penali	polizia locale, commercio,, anagrafe, contratti
la **qualità** di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale	polizia locale, commercio,

DEFINIZIONI

Art. 4 Banca Dati

qualsiasi complesso **organizzato** di dati personali, ripartito in una o più unità dislocate in uno o più siti

- **BD elettronica / cartacea**

- **BD elettronica: attenzione aggiornamenti/allineamenti**
  definizione profili autorizzazione per lettura/modifica/cancellazione

DEFINIZIONI

Art. 4 Trattamento dati personali

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti:

raccolta registrazione organizzazione
conservazione consultazione elaborazione
modificazione selezione estrazione
raffronto utilizzo interconnessione
blocco comunicazione diffusione
cancellazione distruzione

di dati, anche se non registrati in una banca di dati

DEFINIZIONI

Art. 4 Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DEFINIZIONI

Art. 4 Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

Esempio: pubblicazione albo pretorio; pubblicazione su sito internet

IL PROCESSO PRIVACY

- Principi generali
- Soggetti
- Diritti dell'interessato
- I soggetti pubblici
- Misure di sicurezza

SOGGETTI

Soggetti coinvolti nel trattamento

Titolare
Comune

Cittadino; Dipendente; Fornitore

- Responsabile (*facoltativo*)
- Amministratore di rete / sistema / database
- Incaricato

- Responsabile in outsourcing (*fac.*)
- Interessato
- Incaricato

SOGGETTI

Titolare del trattamento

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

SOGGETTI

Titolare del trattamento

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

SOGGETTI

Responsabile del trattamento

figura facoltativa

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Responsabile "interno"

Responsabile "in outsourcing" in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del Titolare

SOGGETTI

Responsabile del trattamento

Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza

Possono essere designati responsabili più soggetti

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e delle proprie istruzioni

SOGGETTI

Responsabile del trattamento in outsourcing

Esempi di Responsabili del trattamento “in outsourcing”:

•Medico del lavoro

•Tesoreria

•Soggetto esterno incaricato dell’erogazione di servizi alla persona

•Soggetto esterno incaricato di elaborazioni informatiche

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

L’amministratore di sistema è colui che:

- gestisce e manutiene un impianto di elaborazione
- amministra banche di dati
- amministra reti
  amministra apparati di sicurezza
  amministra sistemi software complessi

Possono essere uno o più amministratori

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

L’amministratore di sistema è colui che:

•custodisce le credenziali
• gestisce sistemi di autenticazione
• gestisce sistemi di autorizzazione
• realizza copie di sicurezza (backup e recovery)

E’ un incarico di natura fiduciaria che richiede requisiti tecnico-organizzativi, di onorabilità, professionalità e moralità

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

La nomina dell'amministratore di sistema deve portare i titolari a valutare la capacità, l'esperienza e l'affidabilità del soggetto designato.

L'attività degli amministratori di sistema deve essere verificata con cadenza almeno annuale.

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad esse attribuite, devono essere riportati sul documento programmatico sulla sicurezza.

La designazione deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

Quando l'attività dell'amministratore di sistema riguarda il trattamento di dati personali di lavoratori,il titolare è tenuto a rendere nota l'identità dell'amministratore attraverso:

- l'informativa agli interessati art.13
- il disciplinare tecnico provv. N°13 del 1 marzo 20 07
- intranet
- ordini di servizio
- circolari

SOGGETTI

Amministratore di sistema

Provvedimento a carattere generale 27 novembre 2008 -

La criticità del ruolo di amministratore di sistema deve portare i titolari ad adottare idonee cautele per prevenire e controllare accessi non consentiti ai dati personali.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici con caratteristiche di completezza, inalterabilità, integrità.

Le registrazioni devono comprendere gli eventi e la loro collocazione temporale ed essere mantenute per un minimo di sei mesi.

SOGGETTI

Incaricato del trattamento

Le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare (e/o dal Responsabile, se designato)

- operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite

- la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito

Esempio: il dipendente (o il collaboratore) che per conto della struttura del Titolare elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal Titolare medesimo (e/o dal Responsabile, se designato).

SOGGETTI

Interessato

La persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali

Esempio: se un trattamento riguarda l'indirizzo, il codice fiscale ecc. di Mario Rossi o della XYW Spa, Mario Rossi e la XYW Spa sono rispettivamente gli "interessati"

IL PROCESSO PRIVACY

- Principi generali
- Soggetti
- Diritti dell'interessato
- I soggetti pubblici
- Misure di sicurezza

DIRITTI DELL'INTERESSATO

L'interessato ha diritto di:

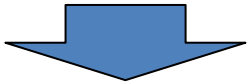
•ottenere informazioni e trattamenti specifici sui dati personali che lo riguardano (cfr. art. 13 – Informativa)

•opporsi al trattamento, per motivi legittimi, dei dati che lo riguardano

•ottenere cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione di legge

DIRITTI DELL'INTERESSATO

I diritti previsti sono esercitati con richiesta rivolta senza formalità al Titolare o al Responsabile, anche per il tramite di un incaricato
Alla richiesta è fornito riscontro senza ritardo



Termine per riscontro: 15 giorni da ricevimento richiesta.
Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, entro 15 giorni dal suo ricevimento il Titolare o il Responsabile ne danno comunicazione all'interessato. In tal caso, il termine è di 30 giorni dal ricevimento della richiesta.

INFORMATIVA ALL'INTERESSATO

Le informazioni che il Titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto, prima di effettuare qualunque trattamento

- contiene informazioni sui diritti dell'interessato
- consente al titolare di trattare lecitamente i dati secondo le disposizioni dell'art. 11
- l'omessa o inidonea informativa all'interessato è punita con la sanzione amministrativa da € 3.000 a 30.000 (art. 161)

INFORMATIVA ALL'INTERESSATO

•le finalità e le modalità del trattamento cui sono destinati i dati

•la natura obbligatoria o facoltativa del conferimento dei dati

•le conseguenze di un eventuale rifiuto di rispondere

•i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi

INFORMATIVA ALL'INTERESSATO

Redigere, per quanto possibile, una prima informativa breve. In linea di massima l'informativa breve, quando è scritta, può avere la seguente formulazione:

"I SUOI DATI PERSONALI:
Utilizziamo - anche tramite collaboratori esterni - i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri suoi diritti, sono riportate su..."

CONSENSO

La libera manifestazione della propria volontà con cui l'interessato accetta espressamente un determinato trattamento dei suoi dati personali, sul quale è stato preventivamente informato da chi gestisce i dati.

Il consenso è documentato in forma scritta; deve essere manifestato in forma scritta se il trattamento riguarda dati sensibili.

CONSENSO

Due “livelli” di consenso

- all’intero trattamento (o ad alcune operazioni) dei dati personali (pertinenti allo scopo della raccolta), per le finalità indicate nell’informativa

- al trattamento di dati personali al fine di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

CESSAZIONE DEL TRATTAMENTO

In caso di cessazione, per qualsiasi causa, di un trattamento i dati possono essere:

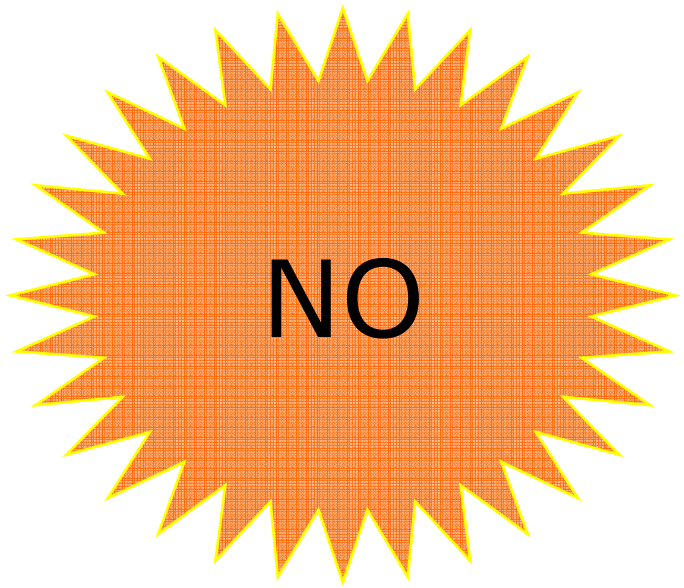
1. distrutti
2. ceduti ad altro titolare (**attenzione alle condizioni previste!**)
3. conservati per fini esclusivamente personali (**attenzione alle condizioni previste!**)
4. conservati (**attenzione alle condizioni previste!**)

IL PROCESSO PRIVACY

- Principi generali
- Soggetti
- Diritti dell'interessato
- I soggetti pubblici
- Misure di sicurezza

I SOGGETTI PUBBLICI

I soggetti pubblici devono richiedere il consenso?



I SOGGETTI PUBBLICI

•ai soggetti pubblici (esclusi gli enti pubblici economici) NON serve il consenso

•qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle **funzioni istituzionali**

•il trattamento di dati personali diversi da quelli sensibili e giudiziari è consentito per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente

I SOGGETTI PUBBLICI

Art. 19 - DATI “COMUNI”
comunicazione ad altri soggetti pubblici

in assenza di norma di legge e di regolamento, è ammessa solo se:

•è necessaria allo svolgimento di funzioni istituzionali

•si effettua comunicazione al Garante e sono decorsi 45 gg. dal ricevimento (da parte del Garante) della comunicazione, salvo diversa determinazione anche successiva del Garante

I SOGGETTI PUBBLICI

Art. 19 - DATI “COMUNI”
comunicazione a privati o enti pubblici economici;
diffusione

sono ammesse solo se previste da norme di legge o regolamento

I SOGGETTI PUBBLICI

Artt. 20, 21 - DATI SENSIBILI / GIUDIZIARI

Il trattamento è consentito solo se autorizzato da espressa disposizione di legge (o provvedimento del Garante) in cui sono specificati:

- i tipi di dati trattabili
- le operazioni eseguibili
- le finalità di rilevante interesse pubblico perseguite

In assenza di individuazione dei dati sensibili / giudiziari e delle operazioni eseguibili nella disposizione di legge, il trattamento è consentito solo adottando un apposito **Regolamento**

I SOGGETTI PUBBLICI

Artt. 20, 21 - DATI SENSIBILI / GIUDIZIARI

Se il trattamento **non** è previsto da una disposizione di legge, è consentito solo:

- se viene richiesta al Garante l'individuazione delle attività, tra quelle demandate dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato (ai sensi dell'art. 26, c. 2) il trattamento dei dati sensibili

I SOGGETTI PUBBLICI

Artt. 22 - DATI SENSIBILI / GIUDIZIARI

I soggetti pubblici trattano solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa

Nell'informativa (art. 13) i soggetti pubblici fanno espresso riferimento alla normativa in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari

I SOGGETTI PUBBLICI

Art. 22 - DATI SENSIBILI / GIUDIZIARI

Gli elenchi, registri o banche di dati in formato elettronico sono trattati:

con tecniche di cifratura

(o) con l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità

I SOGGETTI PUBBLICI

Art. 22 - STATO DI SALUTE / VITA SESSUALE

I dati sono **conservati separatamente** da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Anche quando sono tenuti in elenchi, registri o banche di dati **non** in formato elettronico valgono le modalità di trattamento previste precedentemente per il trattamento di dati sensibili/giudiziari.

I SOGGETTI PUBBLICI

Art. 48: Quando l'autorità giudiziaria può acquisire dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. Gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

I SOGGETTI PUBBLICI

Art. 54: Quando le autorità di P.S. o le forze di polizia possono acquisire dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. Gli uffici interessati possono avvalersi di convenzioni per agevolare la consultazione, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli artt. 3 e 11

Art. 61: Il Garante ha elaborato un codice di deontologia e di buona condotta per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici

IL PROCESSO PRIVACY

- Principi generali
- Soggetti
- Diritti dell'interessato
- I soggetti pubblici
- Misure di sicurezza

MISURE DI SICUREZZA

Sono tutti gli accorgimenti e i dispositivi utilizzati per garantire che:

- i dati non vadano distrutti o persi anche in modo accidentale
- solo le persone autorizzate possano accedere ai dati
- non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti

MISURE DI SICUREZZA

DISPONIBILITÀ
(dei dati)
Garanzia che i dati siano accessibili quando necessario

RISERVATEZZA
Garanzia che i dati siano accessibili solo alle persone autorizzate e preventivamente identificate, che gli accessi siano controllati

INTEGRITÀ
Gestione accurata e completa delle informazioni, salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche

SICUREZZA DEI DATI

MISURE DI SICUREZZA

Le misure di sicurezza individuate dal codice possono essere classificate

Rispetto alle modalità di trattamento:

Trattamenti con strumenti elettronici
Trattamenti con strumenti non elettronici

Rispetto al grado di importanza:

Minime
Idonee

MISURE DI SICUREZZA

Minime

Previste per i trattamenti elettronici e non; il Codice individua le Misure minime, il Disciplinare tecnico (all. “B“ del Codice, aggiornato dal legislatore) ne definisce le modalità di attuazione

La violazione delle misure minime => **sanzioni penali**

Idonee

Definite in relazione a:
- natura dei dati
- progresso tecnico
- caratteristiche del trattamento
- per custodire e controllare i dati

riducendo i principali rischi individuati

La violazione delle misure idonee => **sanzioni civili**

MISURE DI SICUREZZA

Trattamento dati personali con strumenti elettronici

- autenticazione informatica (*es.: user-id + password*)
- adozione di procedure di gestione delle credenziali di autenticazione (*es.: password*)
- utilizzazione di un sistema di autorizzazione (*es.: lettura / scrittura / cancellazione*)
- aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (*es.: lettere nomina incaricati, responsabili/outsourcing*)
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, accessi non consentiti e a determinati programmi informatici (*es.: screen saver, antivirus, firewall, …*)

MISURE DI SICUREZZA

Trattamento dati personali con strumenti elettronici

- adozione di procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi (es.: back-up, piano ripristino)
- redazione e aggiornamento del documento programmatico sulla sicurezza
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

MISURE DI SICUREZZA

Trattamento dati personali senza strumenti elettronici

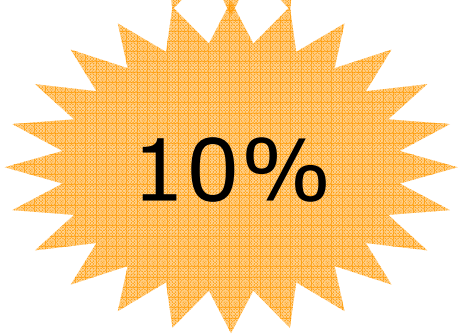
- aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative (*es.: lettere nomina incaricati, responsabili/outsourcing*)
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti (*es.: istruzioni operative*)
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati (*es.: registro accessi ad archivi dati sensibili fuori orario ufficio*)

Sicurezza Informatica

Ambito privacy

Trattamento dati personali
con strumenti elettronici

Trattamento dati personali
senza strumenti elettronici



IL PROCESSO PRIVACY
area informatica

- Rischi
- Sicurezza
- Prevenzione operativa
- Sanzioni

I RISCHI

Le tecnologie dell'informazione e della comunicazione sono utilizzate per:

- Lo snellimento
- L'ottimizzazione
- Una maggiore efficienza dei procedimenti amministrativi

Ciò comporta una serie di "nuovi" rischi

I RISCHI

Sono rischi che possono determinare gravi conseguenze sull'affidabilità dei DATI e dei SERVIZI

I RISCHI

I rischi informatici sono dovuti a:

- Inaffidabilità ed inadeguatezza delle componenti hardware e software
- Possibili intrusioni informatiche

I RISCHI

Un sistema informativo è sicuro se soddisfa, relativamente ai dati, queste condizioni:

- Disponibilità
- Integrità
- Autenticità
- Riservatezza

I RISCHI

DISPONIBILITÁ

L'informazione ed i servizi devono essere disponibili per gli utenti in relazione ai livelli di servizio

AUTENTICITÁ

La provenienza dei dati deve essere garantita e certificata

I RISCHI

RISERVATEZZA

L’informazione può essere conosciuta ed utilizzata solo dal personale autorizzato

DISPONIBILITA’

L’informazione ed i servizi devono essere disponibili per gli utenti in relazione ai livelli di servizio

ANALISI DEL RISCHI

CAUSE DEI RISCHI

Carenze	responsabilità non assegnate, organizzative sottovalutazione dei rischi ecc.
Colpa	causati da non conoscenza o incuria
Dolo	dovuti a interventi fraudolenti voluti

ANALISI DEL RISCHI

ORIGINE DEI RISCHI

Interni	legati all'attività dei dipendenti e dei collaboratori dell'Ente
Esterni	legati all'attività di persone esterne all'Ente
Ambientali	legati ad eventi naturali o al malfunzionamento di strutture circostanti

ANALISI DEL RISCHI

MODALITÁ DEI RISCHI

Denial of service	comandi che pregiudicano la funzionalità delle reti e dei server
Virus	software che ha la capacità di autopropagarsi

L’informatica distribuita e l’utilizzo di internet può aumentare il rischio

IL PROCESSO PRIVACY
area informatica

- Rischi
- Sicurezza
- Prevenzione operativa
- Sanzioni

SICUREZZA

RISCHI ALTI

•Esempio: Quando il possibile danno interessa i dischi di memoria, con conseguente perdita dei dati in essi contenuti.

RISCHI MEDI

Esempio: Quando si ha un blocco totale o parziale del sistema senza danneggiamento dei dischi di memoria.

RISCHI BASSI

Esempio: Quando si ha solo il danneggiamento del software, necessitando una reinstallazione dello stesso.

SICUREZZA

Nell’ambito della sicurezza i rischi possono essere classificati in:

Alti

Medi

Bassi

SICUREZZA

Classificazione della sicurezza:

- Sicurezza fisica
- Sicurezza logica
- Sicurezza organizzativa
- Sicurezza di continuità operativa

SICUREZZA

Sicurezza fisica:

- Proteggere le persone che operano sui sistemi
- Proteggere le aree
- Proteggere le componenti del sistema informativo

SICUREZZA

Sicurezza fisica (di area):

- Protezioni perimetrali dei siti
- Protezione fisica dei supporti
- Controlli degli accessi ai server
- Messa in sicurezza dei locali

SICUREZZA

Sicurezza fisica (hardware):

- Protezioni dai danneggiamenti
- Messa in sicurezza degli impianti (alimentazione, condizionamento)
- Controlli degli accessi
- Manutenzione dell'hardware

SICUREZZA

Sicurezza logica:

- Proteggere le informazioni
- Proteggere i dati
- Proteggere le applicazioni
- Proteggere i sistemi
- Proteggere le reti

SICUREZZA

Sicurezza organizzativa

E’ rappresentata da un insieme di norme e procedure atte a regolamentare gli aspetti organizzativi del processo delle sicurezza

- Definire ruoli, compiti e responsabilità per gestire il processo della sicurezza
- Adottare procedure ad integrare le contromisure tecnologiche attivate
- Sviluppare controlli sulla affidabilità delle apparecchiature

ANALISI DEL RISCHI

MODALITÁ DEI RISCHI

Intercettazioni	attraverso la rete di trasmissione
Ingegneria sociale	con la sola finalità di colpire la vittima
Backdoor	quando vi sono punti di ingresso non noti nel software
Cavalli di troia	con software atto ad operare in modalità non conosciuta

IL PROCESSO PRIVACY
area informatica

- Rischi
- Sicurezza
- Prevenzione operativa
- Sanzioni

PREVENZIONE OPERATIVA

Principali prassi (1):

- *Gestione dei backup
- *Custodia e gestione password
- *Gestione codice identificativo
- *Gestione profili di autorizzazione
- Supporti informatici removibili
- Gestione dischi ottici
- Gestione pen-drive

* misura minima

PREVENZIONE OPERATIVA

Principali prassi (2):

- Gestione PC standalone
- Gestione PC portatili
- *Sicurezza dell'informazione e dei componenti del S.I.
- Dismissione banche dati
- *Controllo accessi
- Gestione antivirus

* misura minima

PREVENZIONE OPERATIVA

Principali prassi (3):

- Installazione nuovi HW e SW
- Gestione banche dati centrali
- Gestione reti informatiche
- *Disaster recovery
- Trasmissione dati via e-mail

* misura minima

PREVENZIONE OPERATIVA

BACKUP

Scopo: garantire il recupero dei dati che sono stati trattati

Ambito di applicazione:

- Applicazioni distribuite
- PC standalone
- PC portatili
- Dati su disco “C”

PREVENZIONE OPERATIVA

BACKUP

Modalità operative:

- Frequenza quotidiana per i server e settimanale per i pc
- Verifica buon esito dell'operazione
- Conservazione dei supporti in luoghi diversi ed in contenitori protetti
- Adozione di un set minimo di supporti per garantire la rotazione
- Backup non sovrascrivibile con cadenza di almeno 10 giorni

PREVENZIONE OPERATIVA

PASSWORD

Scopo: garantire la corretta gestione delle password

Ambito di applicazione:

- Operazioni sulla rete dell'Ente
- Operazioni sulle applicazioni distribuite
- Operazioni su PC portatili
- Operazioni su PC standalone

PREVENZIONE OPERATIVA

PASSWORD

Modalità operative :

- Mantenere la segretezza della password
- Sostituirla ogni 2 mesi per trattamento sia di dati personali che sensibili e giudiziari
- Deve essere composta da almeno 8 caratteri alfanumerici
- Non deve contenere riferimenti riconducibili all'incaricato
- Comunicare immediatamente la perdita di segretezza
- Disattivarla dopo tre mesi di assenza dell'incaricato

PREVENZIONE OPERATIVA

PROFILI DI AUTORIZZAZIONE

Scopo: Indicare le modalità per l'assegnazione e garantire il corretto uso dei codici identificativi

Ambito di applicazione:

- Trattamento dati personali, sensibili, giudiziari
- Incaricato dotato di credenziali di autenticazione
- Per uno specifico trattamento
- Per un insieme di trattamenti

PREVENZIONE OPERATIVA

PROFILI DI AUTORIZZAZIONE

Modalità operative :

- Viene assegnato ad un singolo incaricato o per classi omogenee di incaricati
- Deve essere limitato ai soli dati necessari per il trattamento
- Al cambio di mansioni occorre una richiesta scritta per modificare il profilo di accesso
- Comunicare immediatamente la perdita di segretezza
- Verificare periodicamente le condizioni per mantenere attivi i profili

PREVENZIONE OPERATIVA

SUPPORTI INFORMATICI REMOVIBILI

Scopo: Fornire indicazioni per l'utilizzo di supporti informatici removibili garantendo la riservatezza e la protezione dei dati

Ambito di applicazione:

- Trattamento dati con supporti informatici removibili
- I supporti removibili possono essere utilizzati eccezionalmente e comunque previa adozione delle misure per proteggere i dati personali

PREVENZIONE OPERATIVA

SUPPORTI INFORMATICI REMOVIBILI

Modalità operative :

- I dati vengono memorizzati su di un supporto diverso da quello contenente i dati personali corrispondenti. Se trasportati devono essere collocati in contenitori differenti, impedendo il ricongiungimento delle informazioni

- I dati sensibili e quelli personali possono essere su di un unico supporto solo se trattati con un sistema di criptatura

- É possibile il riutilizzo del supporto solo se non sono più recuperabili i vecchi dati, in caso contrario il supporto deve essere distrutto

PREVENZIONE OPERATIVA

SUPPORTI INFORMATICI REMOVIBILI DI PROVENIENZA ESTERNA

Modalità operative:

- I supporti provenienti da altri pc devono essere verificati, prima dell'utilizzo, con un programma antivirale per garantire l'assenza di virus
- In mancanza di programmi antivirali aggiornati non è possibile utilizzare supporti di provenienza esterna
- É auspicabile l'utilizzo del supporto esterno solo se si conosce l'affidabilità della fonte

PREVENZIONE OPERATIVA

DISCHI OTTICI

Scopo: Indicare le modalità di utilizzo di questi supporti nelle fasi operative e di archiviazione

Ambito di applicazione:

- Trattamento dati utilizzando come supporti di memoria i dischi ottici removibili
- Utilizzo in apparecchiature che gestiscono sia dati che immagini
- Quando la tecnologia informatica richiede l'utilizzo di questi supporti di memoria

PREVENZIONE OPERATIVA

DISCHI OTTICI

Modalità operative:

- Se i dischi risiedono sulle macchine per più giorni è necessario attivare la protezione fisica dell'hardware
- Se i dati sensibili e quelli personali non possono essere scissi è necessaria una maggiore attenzione alle regole di sicurezza
- L'archiviazione dei dischi è soggetta alle medesime regole di conservazione dei supporti di backup

PREVENZIONE OPERATIVA

PEN-DRIVE

Scopo: Indicare come utilizzare questi supporti nelle fasi operative e di trasferimento

Ambito di applicazione:

- Utilizzo come supporto di memoria per il trasferimento dei dati
- Utilizzo per trasferire all'esterno i dati

PREVENZIONE OPERATIVA

PEN-DRIVE

Modalità operative:

- Occorre applicare tutte le regole di sicurezza previste per l'utilizzo di supporti informatici removibili
- É consigliato l'uso di pen-drive dotate di password
- É bene che non vengano utilizzate come strumento di archiviazione se non conservandoli come supporti di backup

PREVENZIONE OPERATIVA

PC STANDALONE

Scopo: Come utilizzare correttamente i pc non legati a reti informatiche dipartimentali o centrali

Ambito di applicazione:

- Si applica a tutti quei pc standalone che contengono dati personali, sensibili, giuridici, genetici.

PREVENZIONE OPERATIVA

PC STANDALONE

Modalità operative:

- gestire la password di amministratore
- gestire la password degli incaricati (modalità non automatica)
- gestire software antivirus con aggiornamento annuale
- gestione della protezione fisica
- gestione dei backup

PREVENZIONE OPERATIVA

PC PORTATILI

Modalità operative:

- gestire la password di amministratore e quella individuale operativa
- i dati sensibili contenuti devono essere oggetto di criptatura
- in alternativa occorre separare i dati sensibili da quelli personali, memorizzati su supporti diversi e conservati in luoghi diversi

PREVENZIONE OPERATIVA

PC PORTATILI

Modalità operative:

- configurare il pc in modo da aggiornare il software antivirus via rete interna
- gestione dei backup
- l'introduzione di policy interne potrebbero essere decise diverse modalità operative a maggiore tutela dei dati personali

PREVENZIONE OPERATIVA

SICUREZZA INFORMAZIONE E COMPONENTI S.I.

Scopo: Verificare che gli strumenti di raccolta ed elaborazione dei dati rispondano alle normative

Ambito di applicazione:

- Si applica alle strutture centrali, ai sistemi dipartimentali ed a tutti i rimanenti strumenti informatici che trattano dati sensibili.

PREVENZIONE OPERATIVA

SICUREZZA INFORMAZIONE E COMPONENTI S.I.

Modalità operative:

- Verifica efficacia delle misure di sicurezza messe in atto
- Verifica delle criticità in essere e delle eventuali conseguenze
- La verifica deve essere periodica e condotta da esperti
- A fronte di difformità, indicare le azioni intraprese per la risoluzione dei problemi

PREVENZIONE OPERATIVA

DISMISSIONE BANCHE DATI

Scopo: Assicurare che la dismissione di banche dati contenenti dati personali e/o sensibili avvenga correttamente

Ambito di applicazione:

- Si applica alle banche dati che non vengono gestite centralmente e che devono essere cancellate dai supporti sui quali sono collocate

PREVENZIONE OPERATIVA

DISMISSIONE BANCHE DATI

Modalità operative:

- verificare la tipologia dei dati contenuti
- essere autorizzati dal responsabile
- cancellare i dati dal supporto informatico
- verificare il buon esito dell'operazione
- in caso di esito negativo, distruggere il supporto
- annotare ed archiviare i parametri dell'intervento

PREVENZIONE OPERATIVA

CONTROLLO ACCESSI

Scopo: Avere un controllo di coloro che hanno avuto accesso a strutture informatiche

Ambito di applicazione:

- Quando non è possibile una completa protezione fisica del sistema
- Quando all'area è consentito l'accesso anche ai non incaricati
- Quando nell'area sono presenti apparecchiature diverse dai sistemi informatici che necessitano interventi di altro personale

PREVENZIONE OPERATIVA

CONTROLLO ACCESSI

Modalità operative in carenza di altri sistemi di controllo:

- Assicurarsi dell'identità e del profilo di autorizzazione di coloro che accedono
- In caso di carenza della protezione fisica, l'accesso dei non addetti è legato alla presenza di uno degli incaricati

PREVENZIONE OPERATIVA

ANTIVIRUS

Scopo: Applicare criteri che consentono la salvaguardia dei software installati e delle banche dati ad essi pertinenti

Ambito di applicazione:

- Riguarda tutti i pc utilizzati per il trattamento di dati sensibili e di dati personali
- Sono esclusi i client per i quali il sistema di protezione viene gestito centralmente ed in modalità automatica

PREVENZIONE OPERATIVA

ANTIVIRUS

Modalità operative:

- Ogni pc deve essere dotato di software antivirus
- Il software deve essere aggiornato con frequenza almeno annuale
- Le licenze d'uso devono essere rinnovate con regolarità
- Deve essere assegnata la responsabilità del rispetto di quanto sopra

PREVENZIONE OPERATIVA

INSTALLAZIONE NUOVI HW E SW

Scopo: Assicurare che l'inserimento di nuove risorse informatiche non alteri la sicurezza del sistema

Ambito di applicazione:

- Riguarda i pc, i software applicativi, i software di base e d'ambiente, apparecchiature per l'archiviazione elettronica, dispositivi di rete, ecc. acquisiti direttamente dagli utenti per l'inserimento in applicazioni distribuite.

PREVENZIONE OPERATIVA

INSTALLAZIONE NUOVI HW E SW

Modalità operative:

- Comunicare al gestore del sistema gli estremi degli strumenti che si vogliono acquisire
- Verifica della congruità tecnica con il sistema in essere
- In caso di congruità negativa ricercare soluzioni alternative
- Verificare che i nuovi strumenti rispettino le norme privacy

PREVENZIONE OPERATIVA

BANCHE DATI CENTRALI

Scopo: Salvare in banche dati centrali i dati elaborati su pc da parte degli incaricati garantendo la sicurezza dei dati stessi

Ambito di applicazione:

- Riguarda tutti quei dati personali e sensibili che vengono elaborati e non possono risiedere sul “disco c” del pc ed ai quali può anche avere accesso più di un operatore.

PREVENZIONE OPERATIVA

BANCHE DATI CENTRALI

Modalità operative:

- Attivare le banche dati in relazione alle necessità dell'utente
- Definire le autorizzazioni all'accesso
- Definire i formati utilizzabili
- Individuare i referenti responsabili delle cartelle e dei dati in esse contenuti

PREVENZIONE OPERATIVA

RETI INFORMATICHE

Scopo: Garantire il mantenimento della sicurezza del sistema rete

Ambito di applicazione:

- Riguarda tutti quei sistemi che sono gestiti attraverso reti locali a livello di applicazioni distribuite

PREVENZIONE OPERATIVA

RETI INFORMATICHE

Modalità operative:

- gestire l'accesso alla rete con riconoscimento degli utenti
- gestire password utenti
- gestire i sistemi antivirus
- gestire la protezione fisica
- gestire i backup

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Scopo: Ripristinare, a fronte di un grave danneggiamento, l'attività dei server e recuperare i dati contenuti nel sistema

Ambito di applicazione:

- Riguarda gli apparati server in dotazione classificati in:
  - server ad alto impatto per i quali occorre garantire il funzionamento in continuo
  - server di supporto senza necessità di funzionamento in continuo

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Modalità operative:

- Si hanno attività di prevenzione e ripristino quali:
  - analisi dei rischi
  - prevenzione attiva
  - prevenzione passiva
  - ripristino in caso di crash

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Modalità operative (analisi dei rischi):

- Analizzare i rischi fisici come : guasti all'impianto di alimentazione, allagamenti d incendi, surriscaldamento dei locali, guasti hardware endogeni

- Analizzare i rischi logici come : programmi maligni, attacchi alla rete informatica

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Modalità operative (prevenzione attiva):

- -Si hanno attività di prevenzione quali:
  - collocare gli apparati in ambiente controllato
  - adottare generatori e gruppi di continuità per garantire la continuità di alimentazione (verifica funzionalità)
  - climatizzare i locali server (verifica funzionalità)
  - adottare sistemi antincendio (verifica funzionalità)

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Modalità operative (prevenzione passiva):

- Si hanno attività di prevenzione quali:
  - effettuare periodicamente un back-up completo dei database
  - attivare l'assistenza hardware
  - attivare l'assistenza sistemistica
  - attivare l'assistenza software
  - effettuare manutenzione ordinaria hardware e software almeno due volte all'anno

PREVENZIONE OPERATIVA

DISASTER RECOVERY

Modalità operative (ripristino in caso di crash):

- Attivare il processo di intervento degli operatori interessati
- Attivare il processo di ripristino per danno grave all'hardware (coinvolgimento dei dischi)
- Attivare il processo di ripristino per danno lieve all'hardware (senza coinvolgimento dei dischi)
- Attivare il processo di ripristino del software di base
- Attivare il processo di ripristino del software applicativo

PREVENZIONE OPERATIVA

TRASMISSIONE DATI VIA E-MAIL

Scopo: Garantire la ricezione e l'invio in particolare di dati sensibili nel rispetto della normativa privacy

Ambito di applicazione:

- Riguarda tutti coloro che utilizzano la posta elettronica come strumento di comunicazione sia per l'interno che per l'esterno dell'Ente

PREVENZIONE OPERATIVA

TRASMISSIONE DATI VIA E-MAIL

Modalità operative:

- Non è consentito comunicare informazioni classificate come riservate o dati sensibili tramite e-mail e/o web, a meno di:
  - applicare un processo di criptatura
  - inviare separatamente i dati sensibili da quelli personali
  - richiedere una ricevuta di corretto ricevimento dei dati
  - attenzione all'invio a destinatari plurimi (Ccn)

PREVENZIONE OPERATIVA

TRASMISSIONE DATI VIA E-MAIL

Modalità operative:

- Nel caso di ricevimento di mail è opportuno:
  - verificare l'identità del mittente
  - utilizzare con attenzione la funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato a più di un destinatario

IL PROCESSO PRIVACY
area informatica

- Rischi
- Sicurezza
- Prevenzione operativa
- Sanzioni

SANZIONI

ART. 615 – ter Accesso abusivo ad un sistema informatico

Un pubblico ufficiale od un incaricato di un pubblico servizio è soggetto a sanzioni a fronte di:

- accesso abusivo ad un sistema informatico o telematico di interesse pubblico (reclusione da 1 a 5 anni)

- se il fatto avviene con violenza a cose o persone, essendo palesemente armato (reclusione da 3 a 8 anni)

SANZIONI

ART. 615 – quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici

Un pubblico ufficiale od un incaricato di un pubblico servizio è soggetto a sanzioni a fronte di:

- detenzione e diffusione abusiva di codici di accesso a sistemi informativi informatici o telematici al fine di procurare un profitto per sé o ad altri o di arrecare ad altri un danno (reclusione sino ad un anno e multa sino a € 5.164)

SANZIONI

ART. 615 – quinquies Diffusione di dispositivi o programmi informatici diretti a danneggiare un sistema informatico

Un pubblico ufficiale od un incaricato di un pubblico servizio è soggetto a sanzioni a fronte di:

- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare od interrompere totalmente o parzialmente un sistema telematico od informatico (reclusione sino ad 2 anni e multa sino a € 10.329)

SANZIONI

ART. 616 Violazione, sottrazione e soppressione di corrispondenza

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

- Prende conoscenza di corrispondenza chiusa od aperta a lui non destinata. Ovvero la distrugge o sopprime (reclusione sino ad 1 anni e multa sino a € 516)
- Se senza giusta causa rivela in tutto od in parte il contenuto (reclusione sino a 3 anni , è punibile a querela della persona offesa)

Per 'corrispondenza' si intende quella epistolare,telegrafica , telefonica, informatica o telematica, con ogni altra forma di comunicazione a distanza

SANZIONI

ART. 635-bis Danneggiamento di informazioni,dati e programmi informatici

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui , (reclusione da 6 mesi sino a 3 anni , è punibile a querela della persona offesa)

Se il fatto è commesso con abuso della qualità di operatore del sistema (reclusione da 1 sino a 4 anni , si procede d'ufficio)

SANZIONI

ART. 635-ter Danneggiamento di informazioni,dati e programmi informatici utilizzati dallo Stato, da enti pubblici

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità (reclusione da 1 sino a 4 anni)

Se dal fatto deriva la distruzione, deterioramento, cancellazione, alterazione o soppressione delle informazioni, dati o programmi informatici(reclusione da 3 sino a 8 anni)

Se è commesso con abuso della qualità di operatore del sistema la pena è aumentate

SANZIONI

ART. 635-quater Danneggiamento di sistemi informatici o telematici

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

Chiunque, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende in tutto od in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento (reclusione da 1 sino a 5 anni)

Se è commesso con abuso della qualità di operatore del sistema la pena è aumentate

SANZIONI

ART. 635-quinquies

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

Chiunque, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende in tutto od in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento rendendoli inservibili (reclusione da 1 sino a 5 anni)

Se è commesso con abuso della qualità di operatore del sistema la pena è aumentate

SANZIONI

ART. 640-ters Frode informatica

Un pubblico ufficiale od un incaricato di un pubblico sevizio è soggetto a sanzioni a fronte di:

Alterazione del funzionamento del sistema informatico o telematico o intervenendo senza diritto su dati, informazioni o programmi, procura a sé o ad altri un ingiusto profitto con altrui danno, (reclusione da 6 mesi sino a 3 anni e multa sino a
€ 1032)

Se è commesso con abuso della qualità di operatore del sistema la pena è aumentate(reclusione da 1 sino a 5 anni e multa sino a € 1549)

PREVENZIONE OPERATIVA

Titolo Slide 1

- Testo testo uno
- Testo testo due
- Testo testo tre