# Profili di responsabilità nell'uso delle risorse informatiche

Corso di formazione sulla sicurezza Informatica

Arcetri (FI) - 4.11.2015

Eleonora Bovo – Servizio Legale e Contenzioso INFN

# Il fondamento della responsabilità per i pubblici dipendenti

- Art. 28 Costituzione
  I funzionari ed i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili secondo le leggi penali, civili e amministrative, degli atti compiuti in violazione dei diritti. In tali casi la responsabilità civile si estende allo Stato e agli enti pubblici.

# “… funzionari e dipendenti …”?

- Sono tali ai fini della responsabilità non solo i dipendenti in senso stretto, ma anche le persone funzionalmente legate alla Pubblica Amministrazione (P.A.) da un rapporto di servizio.

# Da cosa origina la responsabilità?

- La responsabilità del dipendente pubblico – nelle articolazioni che vedremo – deriva dall'inadempimento dei doveri che nascono dal rapporto di pubblico impiego

# I diversi profili della responsabilità

- PENALE: quando la condotta ha le caratteristiche proprie del reato. La responsabilità penale è personale ed esclude la responsabilità civile della PA per i danni cagionati a terzi ove si tratti di attività poste in essere con dolo, per finalità egoistiche e per fini estranei a quelli istituzionali dell'ente
- DISCIPLINARE: :quando la condotta viola doveri funzionali individuati nel codice disciplinare

# I diversi profili della responsabilità

- AMMINISTRATIVA: quando la condotta violativa di norme determina un danno patrimoniale diretto a carico della PA
  - Danno d'immagine
  - Danno da disservizio

- CIVILE: quando la condotta determina un danno a carico di un terzo.

# Evoluzione del concetto di responsabilità civile

- Quando è stata adottata la Carta Costituzionale, si riteneva che i dipendenti dovessero rispondere sempre per *"qualunque fatto doloso o colposo che recasse ad altri un danno ingiusto …"*
- Nel 1957 il Testo Unico degli impiegati civili dello Stato introduce un criterio di imputazione soggettiva più attenuato: il danno arrecato dal dipendente è qualificabile come ingiusto solo se commesso con DOLO o COLPA GRAVE

# Danno: responsabilità del dipendente e della PA

- In caso di danno commesso dal pubblico dipendente il danneggiato può agire in via risarcitoria:
  - nei confronti della Pubblica Amministrazione (in virtù dello stesso art. 28 Costituzione che estende la responsabilità allo Stato e agli enti pubblici datori di lavoro) oppure
  - nei confronti del dipendente autore dell'illecito

# Danno: responsabilità del dipendente e della PA

- Se il danneggiato agisce nei confronti della PA, questa può rivalersi verso il dipendente, ma soltanto se il danno è stato causato con dolo o colpa grave
- L'Amministrazione NON PUO' agire in rivalsa nei confronti del dipendente se questi ha commesso il danno con COLPA LIEVE

# Responsabilità nell'uso delle risorse informatiche

- Se la responsabilità origina dall'inadempimento di doveri connessi all'attività della PA ed al rapporto di lavoro pubblico è necessario, per quanto ci riguarda, censire le norme dettate in relazione all'uso delle risorse informatiche nella Pubblica Amministrazione o almeno individuarne i principi cardine.
- La conoscenza di principi e norme ci consente di adeguare il nostro comportamento alla condotta richiesta e porci al riparo, o comunque ridurre il rischio di incorrere in responsabilità.

# Il quadro normativo

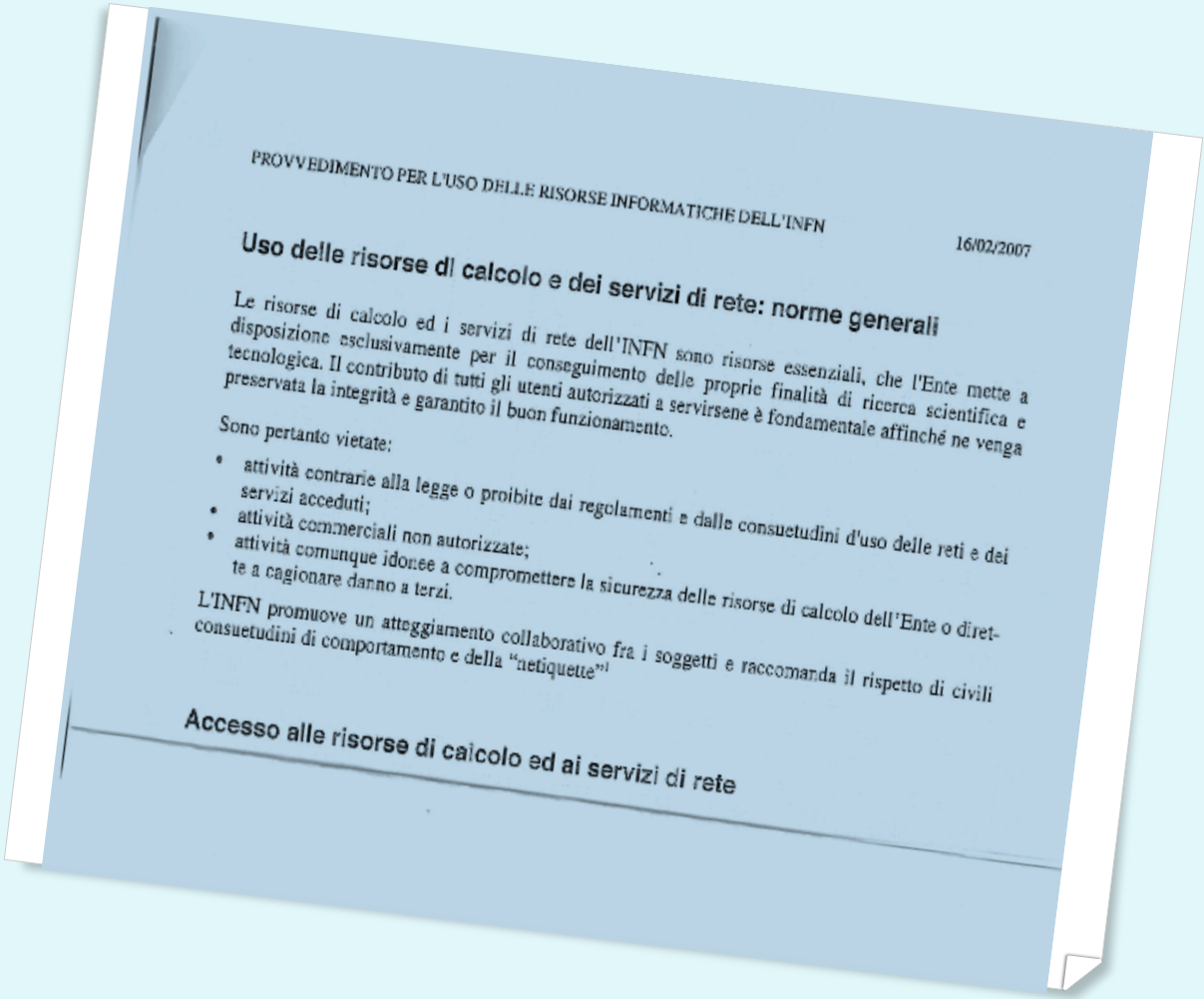
- NORME INTERNE: Norme per l'accesso e l'uso delle risorse informatiche nell'INFN adottate, unitamente alla Carta per la sicurezza informatica INFN, con delibera C.D. n. 10033 del 23.2.2007
- NORME ESTERNE
  - Direttive Europee
  - Codice dell'Amministrazione Digitale (CAD) adottato con D.Lgs. n. 82/2005
  - Codice in materia di protezione dei dati personali (Codice Privacy) di cui al D.Lgs. n. 196/2003
  - Provvedimenti del Garante Privacy con valore prescrittivo

# Norme per l'uso delle risorse informatiche INFN

- individuano:
  - Le **risorse** da salvaguardare
  - I **soggetti** chiamati ad adottare comportamenti idonei alla salvaguardia delle risorse ed in particolare:
    - Utente
    - Amministratore di Sistema
    - Servizio Calcolo e Reti
    - Direttore di Struttura
    - Referenti di gruppi di utenti

# Norme per l'uso delle risorse informatiche INFN

Dettano norme generali per tutti coloro che utilizzano risorse informatiche dell'INFN …



PROVVEDIMENTO PER L'USO DELLE RISORSE INFORMATICHE DELL'INFN 16/02/2007

**Uso delle risorse di calcolo e dei servizi di rete: norme generali**

Le risorse di calcolo ed i servizi di rete dell'INFN sono risorse essenziali, che l'Ente mette a disposizione esclusivamente per il conseguimento delle proprie finalità di ricerca scientifica e tecnologica. Il contributo di tutti gli utenti autorizzati a servirsene è fondamentale affinché ne venga preservata la integrità e garantito il buon funzionamento.

Sono pertanto vietate:

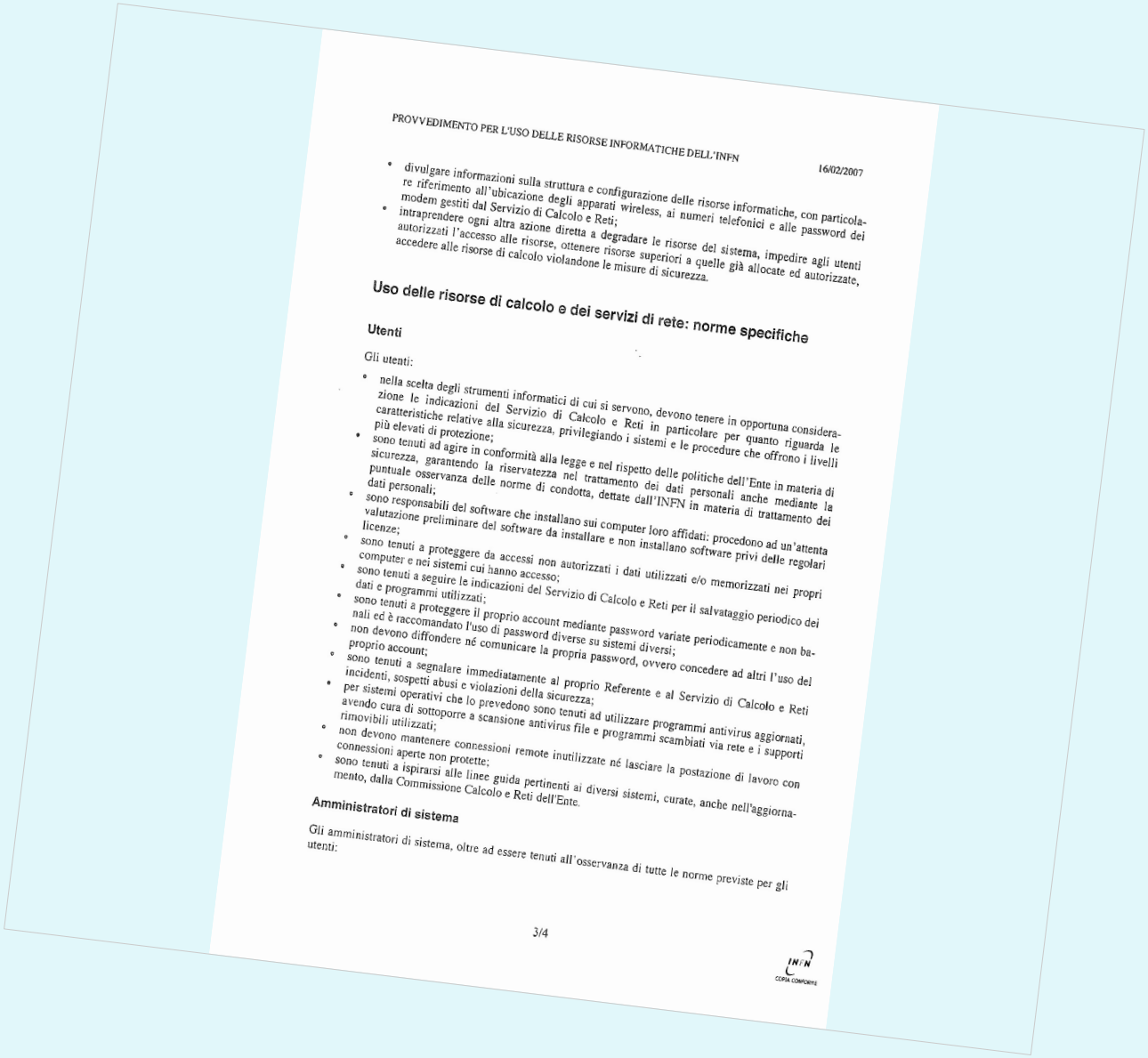
- attività contrarie alla legge o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
- attività commerciali non autorizzate;
- attività comunque idonee a compromettere la sicurezza delle risorse di calcolo dell'Ente o direte a cagionare danno a terzi.

L'INFN promuove un atteggiamento collaborativo fra i soggetti e raccomanda il rispetto di civili consuetudini di comportamento e della "netiquette"[1]

**Accesso alle risorse di calcolo ed ai servizi di rete**

# Norme per l'uso delle risorse informatiche INFN

… e norme specifiche per le singole figure



PROVVEDIMENTO PER L'USO DELLE RISORSE INFORMATICHE DELL'INFN 16/02/2007

- divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento all'ubicazione degli apparati wireless, ai numeri telefonici e alle password dei modem gestiti dal Servizio di Calcolo e Reti;
- intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire agli utenti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle già allocate ed autorizzate, accedere alle risorse di calcolo violandone le misure di sicurezza.

**Uso delle risorse di calcolo e dei servizi di rete: norme specifiche**

**Utenti**

Gli utenti:

- nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio di Calcolo e Reti in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;
- sono tenuti ad agire in conformità alla legge e nel rispetto delle politiche dell'Ente in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali anche mediante la puntuale osservanza delle norme di condotta, dettate dall'INFN in materia di trattamento dei dati personali;
- sono responsabili del software che installano sui computer loro affidati: procedono ad un'attenta valutazione preliminare del software da installare e non installano software privi delle regolari licenze;
- sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;
- sono tenuti a seguire le indicazioni del Servizio di Calcolo e Reti per il salvataggio periodico dei dati e programmi utilizzati;
- sono tenuti a proteggere il proprio account mediante password variate periodicamente e non banali ed è raccomandato l'uso di password diverse su sistemi diversi;
- non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
- sono tenuti a segnalare immediatamente al proprio Referente e al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza;
- per sistemi operativi che lo prevedono sono tenuti ad utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati;
- non devono mantenere connessioni remote inutilizzate né lasciare la postazione di lavoro con connessioni aperte non protette;
- sono tenuti a ispirarsi alle linee guida pertinenti ai diversi sistemi, curate, anche nell'aggiornamento, dalla Commissione Calcolo e Reti dell'Ente.

**Amministratori di sistema**

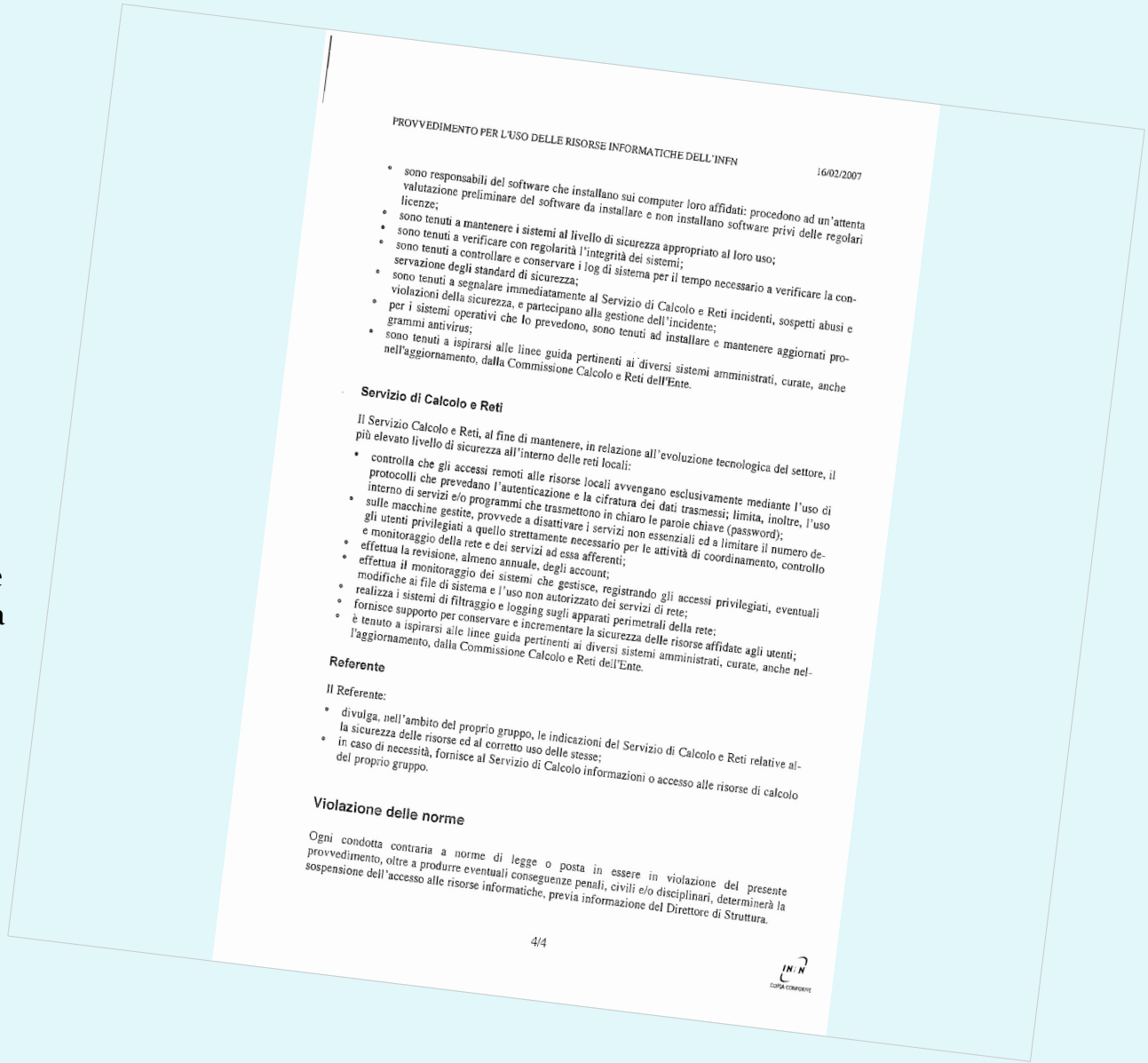
Gli amministratori di sistema, oltre ad essere tenuti all'osservanza di tutte le norme previste per gli utenti:

3/4

# Norme per l'uso delle risorse informatiche INFN

… e norme specifiche per le singole figure

Tali norme sono attualmente in corso di aggiornamento da parte del gruppo di lavoro Harmony



PROVVEDIMENTO PER L'USO DELLE RISORSE INFORMATICHE DELL'INFN 16/02/2007

- sono responsabili del software che installano sui computer loro affidati: procedono ad un'attenta valutazione preliminare del software da installare e non installano software privi delle regolari licenze;
- sono tenuti a mantenere i sistemi al livello di sicurezza appropriato al loro uso;
- sono tenuti a verificare con regolarità l'integrità dei sistemi;
- sono tenuti a controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
- sono tenuti a segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza, e partecipano alla gestione dell'incidente;
- per i sistemi operativi che lo prevedono, sono tenuti ad installare e mantenere aggiornati programmi antivirus;
- sono tenuti a ispirarsi alle linee guida pertinenti ai diversi sistemi amministrati, curate, anche nell'aggiornamento, dalla Commissione Calcolo e Reti dell'Ente.

**Servizio di Calcolo e Reti**

Il Servizio Calcolo e Reti, al fine di mantenere, in relazione all'evoluzione tecnologica del settore, il più elevato livello di sicurezza all'interno delle reti locali:

- controlla che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi; limita, inoltre, l'uso interno di servizi e/o programmi che trasmettono in chiaro le parole chiave (password);
- sulle macchine gestite, provvede a disattivare i servizi non essenziali ed a limitare il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento, controllo e monitoraggio della rete e dei servizi ad essa afferenti;
- effettua la revisione, almeno annuale, degli account;
- effettua il monitoraggio dei sistemi che gestisce, registrando gli accessi privilegiati, eventuali modifiche ai file di sistema e l'uso non autorizzato dei servizi di rete;
- realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete;
- fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti;
- è tenuto a ispirarsi alle linee guida pertinenti ai diversi sistemi amministrati, curate, anche nell'aggiornamento, dalla Commissione Calcolo e Reti dell'Ente.

**Referente**

Il Referente:

- divulga, nell'ambito del proprio gruppo, le indicazioni del Servizio di Calcolo e Reti relative alla sicurezza delle risorse ed al corretto uso delle stesse;
- in caso di necessità, fornisce al Servizio di Calcolo informazioni o accesso alle risorse di calcolo del proprio gruppo.

**Violazione delle norme**

Ogni condotta contraria a norme di legge o posta in essere in violazione del presente provvedimento, oltre a produrre eventuali conseguenze penali, civili e/o disciplinari, determinerà la sospensione dell'accesso alle risorse informatiche, previa informazione del Direttore di Struttura.

4/4

# Necessaria focalizzazione su alcuni temi

- Data l'impossibilità di esaminare tutto il complesso normativo che disciplina l'uso delle risorse informatiche in una Pubblica Amministrazione concentreremo l'attenzione sul tema della sicurezza e gli adempimenti richiesti alle figure professionali tenuti a salvaguardarla

# Le esigenze di sicurezza informatica

- Sia il Codice dell'Amministrazione Digitale che il Codice Privacy e la Carta della Sicurezza Informatica INFN richiedono l'adozione di **misure di sicurezza idonee e preventive** (art. 51 CAD e art. 31 Codice privacy) per il trattamento di dati con strumenti informatici

# Le esigenze di sicurezza informatica e l'Amministratore di Sistema

- Il Garante Privacy, con provvedimento del 27.11.2008, ha constatato la particolare rilevanza degli Amministratori di sistema nel garantire la sicurezza dei sistemi e dei dati personali trattati, li ha individuati nelle *"figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti"* oltre alle *"figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di software complessi"*

# L'Amministratore di sistema

- Ricopre un ruolo di particolare rilevanza, specificità e criticità nell'ambito della sicurezza dei sistemi e dei dati
  - In ambito di tutela dei dati personali ad es. gran parte dei compiti previsti nell'Allegato B al Codice Privacy (quali le operazioni di backup e recovery dei dati, la custodia delle credenziali, la gestione dei sistemi di autenticazione e di autorizzazione …) spettano all'A.d.S.

# L'Amministratore di sistema

- Nell'INFN le direttive già fornite per l'individuazione di questa figura professionale sono oggetto di aggiornamento. Il gruppo Harmony sta lavorando alla revisione dello schema di designazione ed alle informative.

# L'Amministratore di sistema:
## individuazione

- Deve essere individuato previa valutazione dell'esperienza della capacità e dell'affidabilità
- Deve fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza
- Deve essere individuato tenendo conto di criteri di valutazione equipollenti a quelli richiesti per la designazione di un responsabile del trattamento (art. 29 Codice Privacy)

# L'Amministratore di sistema:
## individuazione

- Deve essere designato in modo individuale con indicazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
- I dati identificativi degli A.d.S. e le funzioni ad essi attribuite devono essere riportati in un documento interno da mantenere aggiornato
- L'identità degli A.d.S. che si occupino di servizi che trattano o che consentono il trattamento di dati dei lavoratori devono essere resi noti nell'ambito dell'organizzazione (con informativa nell'ambito del rapporto di lavoro o con altri strumenti di comunicazione interna)

# L'Amministratore di Sistema

## compiti

- Principi cardine per il trattamento dei dati personali:
  - I dati devono essere trattati in modo lecito e secondo correttezza
  - Raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni 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 trattati
  - **Conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore agli scopi per i quali sono raccolti o trattati**

# L'Amministratore di sistema

## verifica dell'attività

- L'attività degli A.d.S. deve essere oggetto di verifica almeno annuale circa la rispondenza delle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti di dati effettuati
- Devono registrarsi gli accessi logici degli A.d.S. ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità; devono contenere i riferimenti temporali e l'evento cui si riferiscono e *"devono essere conservate per un congruo periodo non inferiore a sei mesi"*

# Quale è il tempo di conservazione dei dati?

- Non è indicato dalle norme un periodo netto o definito (come è invece prescritto per i fornitori di servizi di comunicazione elettronica); il periodo di conservazione deve essere individuato in modo **congruo con il raggiungimento di finalità definite** (organizzative e sicurezza)

# Qualche dettaglio in più sugli obblighi di sicurezza

- Art. 31 Cod. Privacy e 51 CAD
  - I dati personali  ed i documenti informatici delle pubbliche amministrazioni devono essere 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, di trattamento non consentito o non conforme alle finalità della raccolta

# Obblighi di sicurezza

- Il trattamento con strumenti elettronici è consentito solo dopo aver adottato le seguenti misure minime di sicurezza
  - Autenticazione informatica
  - Procedure di gestione delle credenziali di autenticazione e sistemi di autorizzazione
  - Aggiornamento dell'ambito di trattamento consentito ai singoli incaricati
  - Protezione degli strumenti elettronici e dei dati rispetto ai trattamenti illeciti ad accessi non consentiti ed a particolari programmi informatici
  - Procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei sistemi

# Inadempimento degli obblighi di sicurezza

- Conseguenze ai sensi dell'art. 169 del Codice Privacy con un termine  per la regolarizzazione non superiore a sei mesi
- Conseguenze ai fini risarcitori con responsabilità oggettiva: per evitare di essere condannati al risarcimento è necessario dar prova di aver adottato tutte le misure idonee ad evitare il danno

# Amministrazione dei sistemi e violazioni commesse da utenti

- Uso illecito/illegittimo di risorse web:
  - Violazione del diritto d'autore
  - Condotte diffamatorie o altre illegittimità

- In base al principio di correttezza e di trasparenza è necessario che il datore di lavoro indichi in un Disciplinare, in modo chiaro e particolareggiato e conformemente a quanto stabilito dallo Statuto dei Lavoratori, quali siano le corrette modalità di utilizzo degli strumenti messi a disposizione e se e in che modo vengano effettuati controlli sull'uso degli stessi

# Amministrazione dei sistemi e violazioni commesse da utenti

- E' necessario:
  - Rispettare il principio di necessità di raccolta dati (il datore di lavoro è tenuto a promuovere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri)
  - Rispettare i principi di pertinenza e non eccedenza
  - Minimizzare l'uso dei dati riferibili ai lavoratori
  - Adottare misure tecnologiche volte a minimizzare l'uso di dati identificativi (PETs – Privacy Enhancing Tecnologies)
  - Individuare tempi di conservazione dei dati strettamente limitati al perseguimento di finalità organizzative, produttive e di sicurezza

# Amministrazione dei sistemi e violazioni commesse da utenti

- Nell'adozione di  un Disciplinare si deve tenere in conto che in caso di controllo sull'uso degli strumenti informatici deve essere evitata un'interferenza ingiustificata sui diritti e le libertà fondamentali dei lavoratori e dei soggetti esterni
- In caso di evento dannoso possono essere effettuati controlli diretti a verificare comportamenti anomali
- Deve essere effettuato un controllo preliminare su dati aggregati riferite ad una struttura lavorativa o a delle aree
- Il controllo preliminare può concludersi con un avviso generalizzato circa il rilevato utilizzo anomalo
- In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale

# Amministrazione dei sistemi e violazioni commesse da utenti

- Nello stesso disciplinare circa la **conservazione dei dati**
  - Devono prevedersi sistemi software configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet ed al traffico telematico la cui conservazione non sia necessaria
  - La conservazione temporanea dei dati deve essere giustificata da una **finalità specifica e comprovata,** limitata al tempo necessario e predeterminato a raggiungerla. Un prolungamento dei tempi di conservazione può avvenire solo
    - Per esigenze tecniche e di sicurezza particolari
    - Se il dato è indispensabile per la difesa di un diritto in giudizio
    - Se c'è una richiesta dell'Autorità giudiziaria

# Attenzione all'uso del software!

- L'uso di software non autorizzato può determinare responsabilità sia civili che penali
  - Oltre alle richieste risarcitorie dei soggetti titolari del copyright ….
  - … Si può incorrere nella violazione penale per integrare la quale non è più necessario il "fine di lucro" ma basta il "fine di profitto".

# Violazioni di dati ed obblighi del Garante: il data breach

- Provvedimento Garante privacy del 2 luglio 2015
  - Introduce l'obbligo per le Pubbliche Amministrazioni di comunicare al Garante, entro 48 ore dalla conoscenza del fatto, le violazioni che possano avere impatto significativo sui dati personali contenuti nelle proprie banche dati.
  - E' necessario garantire esattezza, integrità e disponibilità di dati contenuti non solo nelle banche dati di interesse nazionali (art. 60 CAD), ma anche in altre banche dati delle PA (quelle caratterizzate da ingente mole di dati, delicatezza delle informazioni e molteplicità dei soggetti autorizzati ad accedervi).

# Violazioni e responsabilità nell'ambito dei servizi cloud

- Attualmente nel nostro ordinamento non abbiamo una normativa che disciplini l'uso del cloud , ma sono interessanti
  - Schede tecniche del Garante Privacy contenenti indicazioni per l'utilizzo consapevole dei servizi cloud
  - Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica amministrazione fornite da DigitPA (ora AgID)

# Violazioni e responsabilità nell'ambito dei servizi cloud

- La Pubblica Amministrazione può assumere la duplice veste di Fornitrice (provider) o di Fruitrice (buyer) di servizi cloud
- Qualunque sia la veste della P.A. l'utilizzo di servizi cloud deve essere studiato sull'esigenza specifica di trattamento e sulle caratteristiche dello stesso con una attenta predisposizione di vincoli che legano le parti. L'AgID consiglia l'impiego di Privacy Level Agreement (PLA)

# Violazioni e responsabilità nell'ambito dei servizi cloud

- Nel caso in cui la PA sia buyer, l'AgID fornisce indicazioni abbastanza chiare circa le esigenze di cui tener conto nel disciplinare di gara e nel capitolato tecnico
- Dalle Raccomandazioni AgID possiamo ricavare spunti utili anche nel caso in cui la PA dia accesso ai servizi cloud: allo stato attuale non abbiamo una disciplina di questa nuova realtà tecnologica

# Gestione delle responsabilità nei servizi cloud

- Elementi di maggiore rilevanza
  - Individuazione dei ruoli (il Provider è titolare o responsabile dei dati?)
  - Individuazione dell'ambito del trattamento: l'importanza dell'informativa
  - Individuazione della composizione e struttura del cloud
  - Ambito di circolazione dei dati
  - Valutazione dei rischi e delle garanzie

# GRAZIE!

Sono qui per le domande!