Attività del gruppo Harmony

Mini Workshop CCR

Trento, 18 Marzo 2016

Membri

Silvia Arezzini

Eleonora Bovo

Roberto Cecchini

Michele Gulmini

Paolo Lo Re

Michele Michelotto

Sandra Parlati

Ettore Ronconi

Stefano Zani

Documenti

- *Disciplinare per l'uso delle risorse informatiche nell'INFN*
  - sostituirà le *Norme generali per l'accesso e l'uso delle risorse informatiche INFN*
- *Privacy Policy* (www.infn.it/privacy)
- *Norme per il trattamento dei dati personali*
- Template
  - *Richiesta di accesso alle risorse di calcolo*
  - *Designazione di Amministratore di Sistema*

Premessa 1/2

Il **Disciplinare** e la **Designazione** elencano gli obblighi a cui sono tenuti i soggetti che a qualunque titolo intervengono su risorse informatiche dell'INFN in qualità di amministratori: di server (ad esempio server di esperimento), anche virtuali, di istanze 'cloud' (in qualunque tipologia), di porzioni di rete, ecc. ecc..

Una volta identificata la risorsa, è il Direttore della Struttura su cui essa si appoggia, che ne consente l'amministrazione al soggetto identificato.

Le nomine sono di solito quadriennali, ma possono essere limitate anche a periodi più brevi, specialmente in presenza di progetti e attività con durate ben identificate.

Premessa 2/2

il **Disciplinare** regolamenta l'uso delle risorse informatiche per i **fini istituzionali** dell'Ente. Quindi, se l'INFN intenderà rendere disponibile a terzi le proprie risorse per fini diversi (diventando ad esempio un fornitore di servizi internet), il loro uso dovrà essere oggetto di una distinta e specifica regolamentazione, diversa da quella in esso contenuta.

Non è il caso attuale, anche se ad oggi può verificarsi l'accesso di terzi nell'ambito di progetti, convenzioni o conto terzi, rientrando tutte queste attività nelle finalità istituzionali.

Diverso sarebbe se si modificasse il quadro odierno. In questo caso, infatti, l'INFN assumerebbe una veste nuova e diversa da quella che gli è riconosciuta dallo Statuto e dovrebbe quindi conformarsi a tutto un complesso di norme al quale attualmente non è assoggettato, in quanto Ente pubblico di ricerca. Tanto per fare un esempio: in materia di dati personali esiste una disciplina molto stringente per gli ISP che dovrebbe essere applicata.

Privacy Policy

Aggiunto il riferimento alle *Norme per il trattamento dei dati personali dell'INFN*

- Modalità del trattamento
- Il Titolare e i Responsabili del trattamento
- Tipologie di dati
- Cooky
- Facoltatività del conferimento dei dati
- Diritti degli interessati
- P3P

Norme per il trattamento dei dati personali nell'INFN

Tipologie di dati

dati personali le informazioni relative a persone fisiche, giuridiche, enti od associazioni, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

dati sensibili i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

dati giudiziari quelli idonei a rivelare provvedimenti di iscrizione nel casellario giudiziale o nell'anagrafe delle sanzioni amministrative dipendenti da reato e i relativi carichi pendenti o la qualità di indagato o di imputato.

Soggetti

Titolare del trattamento è l'Istituto Nazionale di Fisica Nucleare inteso nel suo complesso.

Responsabili del trattamento sono i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle norme in materia di trattamento, ivi compreso il profilo della sicurezza: i *Direttori delle Strutture*, i *Direttori di Direzioni e Servizi dell'Amministrazione Centrale* e il *Responsabile del Servizio di Presidenza INFN.*

Incaricati del trattamento le persone autorizzate a compiere operazioni di trattamento dei dati; tra loro, coloro che provvedono alla gestione e/o manutenzione di impianti di elaborazione sono incaricati alla funzione di **Amministratore di sistema**.

Interessati al trattamento i soggetti cui si riferiscono i dati personali.

Principi generali

L'Istituto Nazionale di Fisica Nucleare consente il trattamento dei dati personali soltanto per lo svolgimento di attività istituzionali.

Ciascuna operazione di trattamento deve essere effettuata riducendo al minimo l'utilizzo di dati personali

I Responsabili del trattamento individuano per iscritto gli **Incaricati** e gli **Amministratori di sistema** ed indicano l'ambito di trattamento consentito a ciascuno.

Gli stessi Responsabili provvedono alla revoca dell'autorizzazione in tutti i casi in cui vengano meno le condizioni che avevano determinato l'autorizzazione.

Comunicazione e diffusione dei dati

La **comunicazione** dei dati personali **ad un altro soggetto pubblico** può essere effettuata quando è prevista da una norma di legge o di regolamento; in mancanza di tale norma può essere effettuata quando è comunque necessaria per lo svolgimento di funzioni istituzionali.

La **comunicazione** a **privati** o ad **enti pubblici economici** e la **diffusione** sono ammessi esclusivamente quando sono previste da una norma di legge o di regolamento.

In ogni caso i dati idonei a rivelare lo stato di salute non possono essere diffusi

Misure minime di sicurezza

Le **misure minime di sicurezza** sono costituite dall'insieme delle misure tecniche ed organizzative che l'INFN è tenuto ad adottare al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

I **Responsabili** del trattamento sono pertanto tenuti ad adottare tutte le misure idonee a ridurre al minimo i rischi sopra indicati e gli **Incaricati** del trattamento sono tenuti ad evitare condotte che possano pregiudicare la riservatezza

Trattamento elettronico

Le risorse informatiche devono essere accessibili tramite modalità che consentano l'individuazione dell'utente (Responsabile o Incaricato) in modo univoco: attraverso un meccanismo di autenticazione che si concretizza, quanto meno, nell'uso di un codice identificativo personale (user-id) e di una parola chiave (password).

Custode delle password

Il Responsabile del trattamento dei dati personali provvede all'individuazione per iscritto di uno o più **Custodi delle password**. Il ruolo di questa figura è quello di garantire la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.

Il custode delle chiavi è in grado di modificare la password dell'incaricato del trattamento poiché è in possesso delle password privilegiate di tutti i sistemi interessati.

Laddove si rendesse necessario intervenire nel computer dell'incaricato assente, il Custode modifica la password e permette la realizzazione dell'intervento necessario. Provvede poi ad informare l'incaricato che, una volta rientrato in servizio, ripristina una nuova password personale da lui solo conosciuta.

Misure di protezione

I Responsabili del trattamento curano che i server disponibili nella propria Struttura siano ancorati a pareti o pavimenti, localizzati in ambienti caratterizzati da accesso controllato (locali chiusi a chiave) e dotati di sistemi di condizionamento, antincendio ed antiallagamento. Le risorse ritenute critiche devono inoltre essere protette mediante l'installazione di sistemi che garantiscano la continuità dell'energia elettrica.

I Responsabili del trattamento provvedono inoltre, anche mediante i Servizi di Calcolo e Reti, affinché siano installati sistemi anti intrusione informatica, facendo in modo che il loro aggiornamento sia effettuato con cadenza almeno semestrale.

I Responsabili del trattamento curano e verificano, tramite i Servizi di Calcolo e Reti, o le ditte che effettuano l'assistenza informatica, che su tutti gli elaboratori siano installati programmi antivirus in grado di fornire anche una protezione in tempo reale. I programmi devono essere configurati in modo da aggiornarsi automaticamente almeno una volta alla settimana.

Al fine di proteggere gli elaboratori da minacce informatiche gli Incaricati del trattamento sono tenuti in ogni caso ad osservare il *Disciplinare per l'uso delle risorse informatiche dell'INFN*

Copie di salvataggio

Gli Incaricati del trattamento sono tenuti ad effettuare il salvataggio (*backup*) dei propri file.

Il backup può essere effettuato, secondo le indicazioni fornite dai Servizi di Calcolo e Reti, su specifici server oppure su dischi, nastri o altri supporti rimovibili.

I supporti rimovibili contenenti le copie di salvataggio devono essere custoditi in armadi chiusi a chiave. Gli stessi supporti non possono essere riutilizzati da altri incaricati, se non dopo che le informazioni in essi contenute siano state rese inintelligibili e comunque non ricostruibili.

Periodicamente, e con frequenza almeno mensile, gli Incaricati sono tenuti ad effettuare prove di ripristino, per verificare la costante adeguatezza delle metodologie adottate e dei supporti di backup utilizzati.

Disciplinare per l'uso delle risorse informatiche nell'INFN

Principi

- Recepimento AUP GARR;
- minimizzazione uso dati personali e identificativi;
- si applica a tutti quelli cui è consentito l'accesso alle risorse di calcolo e ai servizi di rete.

Definizioni

Risorse di calcolo e servizi di rete

- elaboratori e analoghi dispositivi elettronici, stampanti e altre periferiche di proprietà dell'Ente o comunque connesse alla rete dell'Ente;
- apparati e infrastrutture di rete di proprietà dell'Ente o comunque connessi alla rete dell'Ente;
- il servizio di connettività alle reti locali e geografiche con esclusione della mera connettività geografica garantita tramite accordi tra Istituzioni e Federazioni (ad es. Eduroam);
- istanze virtuali di calcolatori o apparati di rete;
- software e dati acquistati, prodotti o pubblicati dall'INFN.

Definizioni

Soggetti coinvolti

- Utente
- Referente di un gruppo di utenti
- Amministratore di sistema
- Servizio di calcolo e reti
- Direttore di struttura

Accesso alle risorse

- Consentito previa autenticazione;
- autorizzazione rilasciata dal Direttore o da un suo delegato per un periodo temporale limitato alla durata del rapporto sulla base del quale è consentita l'attività all'interno dell'INFN;
- l'accesso è **personale**.

Disposizioni generali

- Le risorse informatiche sono rese disponibili esclusivamente per il conseguimento delle finalità istituzionali dell'Ente.
- L'uso per finalità personali è tollerato purché non violi le leggi applicabili e sia compatibile con le norme del presente Disciplinare e di tutte le indicazioni stabilite dall'INFN.

Disposizioni specifiche

- Non interferire con le competenze del SC&R
- Non fornire accessi non autorizzati
- osservare le norme in www.infn.it/privacy
- responsabili dei dati e del software installato
- uso di password non banali

Compiti del 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 e Reti informazioni o accesso alle risorse di calcolo del proprio gruppo.

Compiti dell'Amministratore

- Controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
- non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
- in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
- seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

Uso dei servizi esterni

Il trattamento dei **dati personali**, sia comuni che sensibili, o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo *cloud*, soltanto ove l'INFN abbia **preventivamente verificato** i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento.

Dati sull'uso delle risorse

Il SC&R, **ai fini di controllo della sicurezza e l'ottimizzazione dei sistemi**, raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti.

Questi dati **sono conservati per un periodo non superiore a un anno**.

I log di *proxy server* o altri sistemi di controllo delle sessioni **non devono essere conservate per un periodo superiore a sette giorni**.

Dati sulla posta elettronica

Si registrano: data, ora, indirizzi del mittente e del destinatario e il risultato delle analisi dell'antivirus e antispam

Conservati (anche il backup) per **non oltre un anno**

La casella di posta è disattivata entro i **due mesi successivi** alla scadenza del termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Direttore o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato **entro un anno** dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Direttore ove ne ravvisi specifica esigenza.

Ulteriori misure

L'INFN adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.

Nel caso in cui, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Servizio di Calcolo e Reti esegue, previa informazione agli interessati e salvo i casi di necessità ed urgenza, ulteriori accertamenti e adotta le misure necessarie ad interrompere le condotte dannose o non consentite.

Nei casi di reiterazione di comportamenti vietati e già segnalati o di particolare gravità, il Responsabile del Servizio di Calcolo e Reti adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Direttore di Struttura, che dispone gli ulteriori provvedimenti ai sensi del punto seguente.

Richiesta di accesso alle risorse

E' un template!

Il/La sottoscritto/a ……., nato/a a ..... il ……..., identificato mediante il seguente documento di identità o riconoscimento

…… .....

Procedure di autenticazione

In alternativa

- Consegna del documento cartaceo con apposizione di firma per presa visione da parte dell'utente.
- Click su di un bottone raggiungibile dopo una procedura di autenticazione con uso delle proprie credenziali AAI.
- Scambio di documenti, tra cui la copia di un documento di identità con fotografia, utilizzando un indirizzo di e-mail fornito dal richiedente e riconosciuto come proprio, garantito dall'approvazione di un referente interno autenticato tramite le proprie credenziali AAI.