Applicazione del Codice della Privacy per Incaricati del trattamento dei dati: sicurezza dei sistemi informatici

Principi e adempimenti previsti dalla legge e dal Regolamento di Ateneo

csiaf

Applicazione codice privacy

- Normativa
- Riferimenti informativi
- Codice in materia di dati personali (generalità)
- Regolamenti di Ateneo
- Codice in materia di dati personali (sicurezza e sanzioni)
- Obblighi
- Sicurezza informatica
- Documento Programmatico sulla Sicurezza dello CSIAF

csiaf

Sicurezza dei sistemi informatici

SICUREZZA

=

obbligo quando si ha a che fare con sistemi informatici, reti, servizi di rete e servizi in rete

non può più essere un comportamento spontaneo ma deve adeguarsi a norme e standard

csiaf

Normativa sulla sicurezza: leggi

Normativa che impone vincoli legislativi:

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

Comprensivo di:

- Una serie di decreti di modifica
- Allegato A.4. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici
- All. B: "Disciplinare tecnico in materia di misure minime di sicurezza"

csiaf

Normativa sulla sicurezza: leggi

Altri provvedimenti del Garante della Privacy:

- Lavoro: le linee guida del Garante per posta elettronica e internet - 1 marzo 2007
- "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - 14 giugno 2007

csiaf

Normativa sulla sicurezza: leggi

Altri vincoli legislativi:

- R.D. 22.4.1941 n. 633, D.Lgs. 29.12.1992 n. 518, L. 18.08.2000, n. 248, D. Lgs. 9.4.2003 n. 68, L. 21.5.2004 n. 128 (tutela del diritto d'autore con norme relative alla tutela giuridica dei programmi per elaboratore)
- Legge n. 547 del 1993, che introduce i computer crimes
- D.Lgs. 13.05.98 n. 171 (disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni ed in tema di attività giornalistica)

csiaf

Normativa sulla sicurezza : leggi

Direttiva governativa:

Direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002, emanata dal Dipartimento per l'Innovazione e le Tecnologie (direttiva Stanca):

"Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali"

Comprensiva di:

- All. 1: "Valutazione del livello di sicurezza"
- All. 2: "Base minima di sicurezza"

csiaf

Normativa sulla sicurezza: AIPA/CNIPA

- AIPA: “Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione” (28 ottobre 1999)
- AIPA: “La sicurezza dei servizi in rete - requisiti, modelli, metodi e strumenti” (14 novembre 2001)
- CNIPA: “Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni” (23 marzo 2006)

csiaf

Normativa sulla sicurezza: europa

Indicazioni europee:

- Comunicazione della Commissione al Parlamento Europeo, al Comitato Economico e Sociale e al Comitato delle Regioni: “Sicurezza delle reti e sicurezza dell’informazione: proposta di un approccio strategico europeo” (2001)

- Risoluzione del Consiglio dell’Unione Europea: “su un approccio europeo per una cultura della sicurezza delle reti e dell’informazione”
(n. 2003/C 48/01, del 18 febbraio 2003)

csiaf

Normativa sulla sicurezza: standard

Standard internazionale BS 7799:

- Parte prima: “Information Technology - Code of practice for information security management”
  recepita dalla ISO/IEC 17799:2000

- Parte seconda: “Information security management systems - Specifications with guidance for use”
  fornisce l’insieme di requisiti per implementare un Sistema di Gestione della Sicurezza delle Informazioni

csiaf

Privacy - riferimenti

- Codice in materia di protezione dei dati personali
- Regolamento di attuazione del codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze
- Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del decreto legislativo 196/2003
- Newsletter n. 35 - Speciale trattamento dati personali
- Sito dello CSIAF: Sicurezza ai sensi del Codice in materia di protezione dei dati personali

csiaf

Codice privacy

Parti del Codice Privacy:

I. DISPOSIZIONI GENERALI: trattano tutte le disposizioni e regole del trattamento con riferimento ai settori pubblico e privato

II. DISPOSIZIONI RELATIVE A SPECIFICI SETTORI: disciplina aspetti nuovi (informazione giuridica, atti giudiziari ecc.) e completa la disciplina per aspetti sanitari e controlli sui lavoratori

III. TUTELA DELL'INTERESSATO E SANZIONI: affronta le tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali

csiaf

Codice privacy

Parti del Codice Privacy:

Allegati:

A. Codici deontologici (attività giornalistica, scopi storici, scopi statistici, scopi statistici e scientifici, ambito crediti)
B. Disciplinare tecnico in materia di misure minime di sicurezza
C. Trattamenti in ambito giudiziario e per fini di polizia

csiaf

Codice privacy: dati

Tipi di dati (ai sensi del codice della privacy):

- dati personali: informazioni relative a persone fisiche o giuridiche identificabili con riferimento a qualsiasi altra informazione
- dati identificativi: dati personali che permettono l'identificazione diretta dell'interessato
- dati anonimi: dati che in origine o in seguito al trattamento non possono essere associati ad un interessato

csiaf

Codice privacy: dati

- dati sensibili: dati personali idonei a rivelare:
  - ✓ origine razziale ed etnica,
  - ✓ convinzioni religiose, filosofiche o altro di genere,
  - ✓ opinioni politiche,
  - ✓ adesione a partiti e sindacati,
  - ✓ adesioni ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
  - ✓ dati personali idonei a rivelare stato di salute e vita sessuale.

- dati giudiziari: dati personali idonei a rivelare:
  - ✓ provvedimenti in materia di casellario giudiziale,
  - ✓ anagrafe sanzioni, carichi pendenti,
  - ✓ qualità di imputato o indagato.

csiaf

Codice privacy: dati

Trattamento: qualunque operazione o complesso di operazioni concernenti:

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

csiaf

Codice privacy: dati

Articoli di interesse relativi ai dati:

Art. 3: Principio di necessità nel trattamento dei dati:

il trattamento non necessario è illecito;
i dati personali e identificativi devono essere utilizzati al minimo; deve essere escluso il trattamento dei dati quando si può ottenere lo stesso risultato con dati anonimi o con associazioni che permettono l'identificazione solo in caso di necessità

Art. 11: Modalità del trattamento e requisiti dei dati:

vengono date indicazioni su come i dati oggetto di trattamento devono essere gestiti e mantenuti; altrimenti non possono essere utilizzati

csiaf

Codice privacy: principi

I pilastri della legge:

- Informativa
- Consenso
- Autorizzazione
- Misure di sicurezza
- Diritti dell'interessato
- Notificazione

csiaf

Codice privacy: soggetti

Soggetti con responsabilità

(ai sensi del codice della privacy):

TITOLARE:

chi è destinatario delle norme, ossia la persona fisica, giuridica, la pubblica amministrazione o altro ente a cui compete decidere finalità, modalità del trattamento dei dati personali e gli strumenti utilizzati, compresa la sicurezza

- ✓ Nel caso di persona giuridica, pubblica amministrazione, ente, associazione o organismo è l'entità nel suo complesso
- ✓ Può essere unità o organismo periferico se esercita potere decisionale autonomo

csiaf

Codice privacy: soggetti

RESPONSABILE:

chi sceglie e gestisce, ossia la persona fisica, giuridica, la pubblica amministrazione o altro ente preposto dal titolare mediante delega

- ✓ la designazione è facoltativa
- ✓ possono essere designati più responsabili, anche mediante suddivisione di compiti
- ✓ può essere anche esterno all'ente
- ✓ deve essere scelto fra soggetti che per esperienza, capacità ed affidabilità forniscano idonee garanzie
- ✓ deve attenersi alle istruzioni del titolare, che può vigilare anche con verifiche periodiche sul loro rispetto

csiaf

Codice privacy: soggetti

INCARICATO:

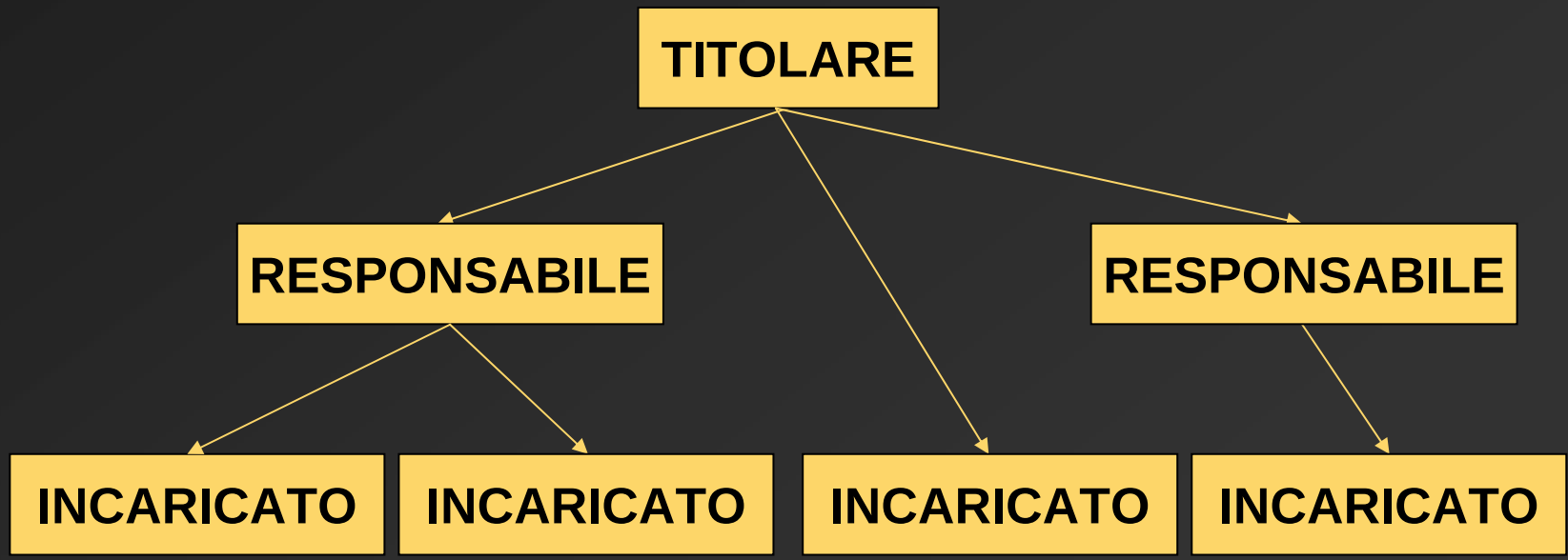
chi accede ai dati per uno scopo lecito a lui delegato, ossia la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile

- ✓ opera sotto l'autorità del titolare o del responsabile
- ✓ deve attenersi alle istruzioni del titolare o del responsabile, che può sorvegliarne l'attuazione
- ✓ può essere designato per documentata preposizione ad una unità per la quale è individuato, per scritto, l'ambito del trattamento consentito agli addetti all'unità medesima

csiaf

Codice privacy: soggetti

Struttura di responsabilità



csiaf

Codice privacy: soggetti

DELEGA:

- deve essere scritta
- deve essere accettata
- conferisce autonomia
- implica controlli ma non ingerenza
- coinvolge il delegato nelle responsabilità

Il delegato può a sua volta delegare se a ciò autorizzato

csiaf

Codice privacy: P.A.

Articoli di interesse relativi ai soggetti pubblici:

Art. 18: Principi sui dati personali:

- il trattamento può essere svolto solo per fini istituzionali

Art. 20 e 22: Principi sui dati sensibili:

- il trattamento può essere svolto solo se autorizzato da disposizioni di legge
- il trattamento può essere svolto solo se impossibile con dati anonimi

csiaf

Regolamento di Ateneo: soggetti

- Regolamento di attuazione del codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze

Titolare dei dati: Università

csiaf

Regolamento di Ateneo: soggetti

Responsabili:

Responsabili delle strutture che detengono i dati personali:

- i responsabili delle unità amministrative;
- i Dirigenti degli uffici dirigenziali dell'amministrazione centrale e di polo, dello SBA, dello CSIAF e del MSN;

csiaf

Regolamento di Ateneo: soggetti

le medesime strutture sono Responsabili anche dei dati personali

- detenuti dallo CSIAF e trattati presso le strutture stesse
- dati in hosting a CSIAF
- ospitati da fornitori di servizi

Ciascun Responsabile può nominare altri Responsabili all'interno della propria struttura
CSIAF può nominare i Responsabili al di fuori della propria struttura, di concerto con i dirigenti di area ed i responsabili delle U.A.

csiaf

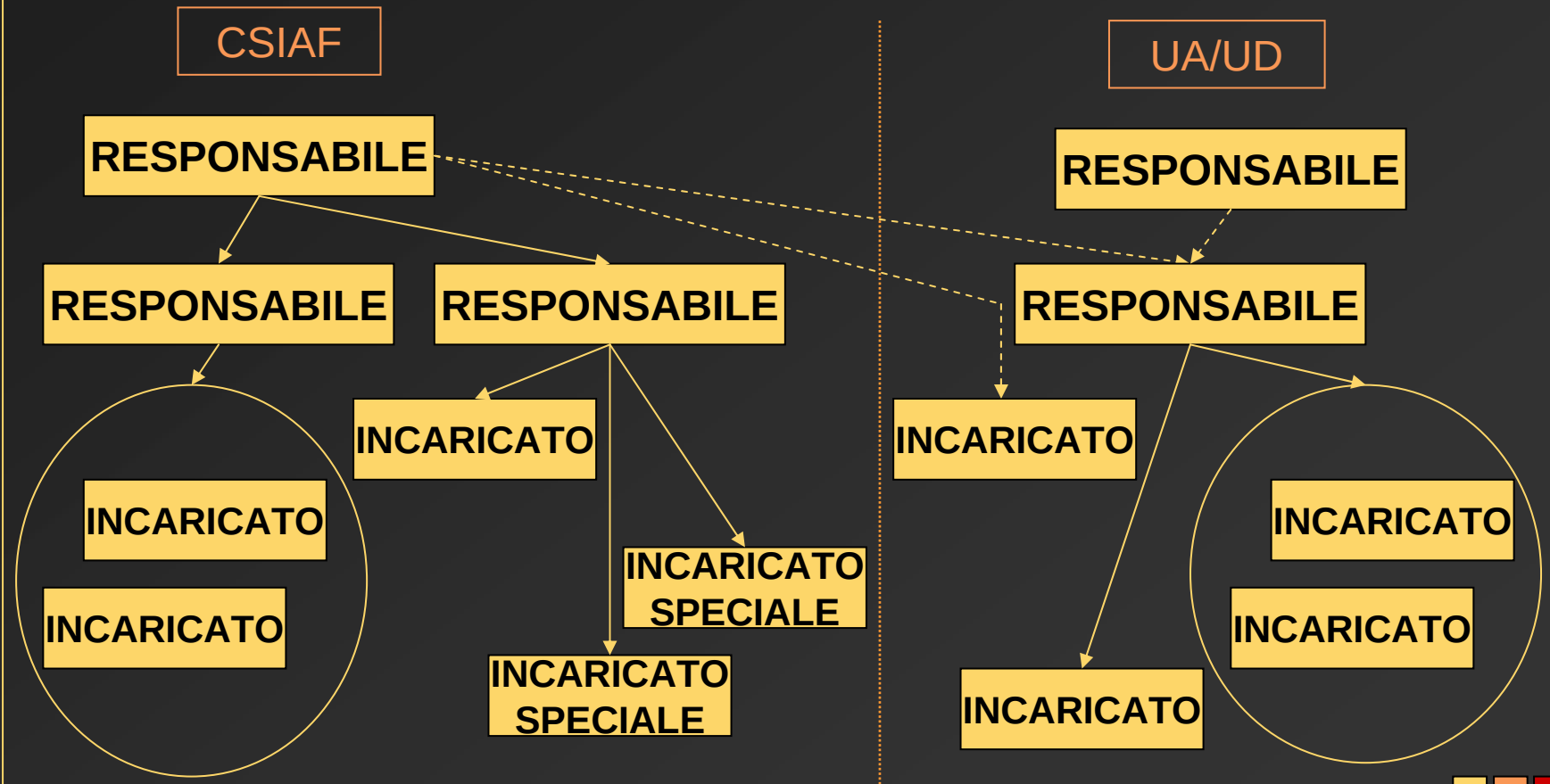
Regolamento di Ateneo: soggetti

Incaricati:

- le nomine sono fatte tipicamente dal Responsabile all'interno della propria struttura
- CSIAF, se non designato un Responsabile, può nominare gli Incaricati al di fuori della propria struttura, d'intesa con i dirigenti di area ed i responsabili delle U.A.
- si possono nominare Incaricati per documentata preposizione (in base al ruolo o funzione svolta)

csiaf

Regolamento di Ateneo: dati CSIAF



csiaf

Regolamento di Ateneo dati sensibili

- Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del decreto legislativo 196/2003

  - deve citare leggi e normative che autorizzano il trattamento
  - deve essere approvato dal Garante
  - è stato fatto su una bozza concordata a cura della CRUI e preventivamente approvata

csiaf

Codice privacy: sicurezza

Articoli di interesse relativi alla sicurezza:

Art. 31: Obblighi di sicurezza

i dati oggetto di trattamento devono essere custoditi e controllati anche in base al progresso tecnico;
devono essere adottate idonee e preventive misure di sicurezza;
occorre ridurre al minimo i rischi di:

- ✓ distruzione o perdita
- ✓ accesso non autorizzato
- ✓ trattamento non consentito o non conforme

Art. 33: Misure minime

comunque è necessario adottare misure minime per assicurare un livello minimo di protezione dei dati

csiaf

Codice privacy: sicurezza

Art. 34: Trattamenti con strumenti elettronici

- il trattamento con strumenti elettronici è consentito solo se si adottano le misure minime previste dal Disciplinare tecnico contenuto nell'allegato alla legge
- le misure minime vengono sinteticamente elencate
- viene sancito l'obbligo di definire e tenere aggiornato un documento programmatico sulla sicurezza

All. B: Disciplinare tecnico in materia di misure minime di sicurezza

- fornisce indicazioni tecniche dettagliate sulle misure minime da adottare

csiaf

Codice privacy: sicurezza

Tipi di misure di sicurezza da adottare:

MISURE MINIME:

le misure da adottare nel trattamento dei dati con strumenti elettronici, indicate dettagliatamente in articoli della legge e nell'allegato "disciplinare tecnico"

MISURE IDONEE:

le misure più stringenti riferite dalla legge, non identificate analiticamente ma identificabili dal titolare o dai responsabili, per ridurre al minimo i rischi: devono essere costantemente aggiornate

csiaf

Codice privacy: sanzioni

Articoli di interesse relativi a conseguenze e sanzioni:

Art. 15: Danni cagionati per effetto del trattamento
responsabilità civili e patrimoniali e casi di necessità di risarcimento

Art. 167: Trattamento illecito di dati
casi di illeciti penali dovuti a violazioni per trarre profitto per sé o per altri o per recare danno ad altri

csiaf

Codice privacy: sanzioni

Art. 168: Falsità nelle dichiarazioni e notificazioni al Garante

caso di illecito penale dovuto a dichiarazioni o notifiche al Garante false

Art. 169: Misure di sicurezza

caso di illecito penale dovuto a mancata adozione delle misure minime di sicurezza

Art. 170: Inosservanza di provvedimenti del Garante

caso di illecito penale dovuto a mancata osservanza di provvedimenti adottati dal Garante in relazione alle garanzie per i dati sensibili

csiaf

Codice privacy: sanzioni

Le misure di sicurezza adottate

hanno un impatto diretto sulle

responsabilità civili e penali

csiaf

Codice privacy: sanzioni

Responsabilità penali:

Le sanzioni penali riguardano le persone fisiche

La mancata adozione delle misure minime comporta un illecito penale

csiaf

Codice privacy: sanzioni

Responsabilità civili e patrimoniali:

I titolari hanno l'obbligo di risarcire gli eventuali danni causati (da loro o dai loro delegati) a terzi in conseguenza del trattamento dei dati personali

Si fa riferimento ad un articolo del c.c. (art. 2050) che parla di danni dovuti allo svolgimento di attività pericolose

Il risarcimento non è dovuto se si dimostra di avere adottato misure idonee ad evitare il danno

csiaf

Codice privacy: obblighi

In base alla legge

31 marzo di ogni anno:

aggiornare il DPS

nella relazione accompagnatoria del bilancio:

riferire sulla avvenuta redazione o aggiornamento del DPS

csiaf

Regolamento di Ateneo: obblighi

In base al regolamento:

- Chiunque voglia intraprendere o cessare il trattamento di dati personali strumentali ad attività didattiche ed organizzative, deve darne previa comunicazione al responsabile della struttura
- I responsabili delle strutture devono comunicare al Titolare, entro il 31 marzo di ciascun anno, l'elenco degli archivi di dati personali attivi e la dichiarazione dell'avvenuta adozione delle misure di sicurezza

csiaf

Regolamento di Ateneo: obblighi

- i responsabili delle strutture che detengono dati personali trattati con strumenti elettronici, entro il 31 marzo di ciascun anno, devono redigere e/o aggiornare il relativo DPS, dandone comunicazione al Titolare

- il Documento Programmatico della Sicurezza di Ateneo è costituito dall'insieme dei Documenti Programmatici delle singole strutture

csiaf

Sicurezza informatica

Obiettivo principale della sicurezza è proteggere i beni informatici

* riducendo i rischi a cui sono esposti
* limitando gli effetti causati dall'eventuale occorrenza di una minaccia (rischio residuo)

con beni informatici si intende:

* sistemi (hw e sw)
* informazioni (banche dati, documenti digitali, dati in transito)
* servizi (posta, accesso a sportelli elettronici)

csiaf

Sicurezza informatica

La sicurezza informatica è l'insieme di misure di carattere

- organizzativo
- tecnologico
- procedurale

mirate ad assicurare la protezione dei beni informatici, conservandone:

- Riservatezza
- Integrità
- Disponibilità

csiaf

Sicurezza informatica

Mezzi per ottenere la sicurezza:

- Implementazione di contromisure (politiche, prassi, procedure, strutture organizzative, funzioni software)
- Formazione del personale sulle politiche di sicurezza

La diffusione di una cultura della sicurezza deve andare in parallelo con l'implementazione delle contromisure

csiaf

Sicurezza informatica

Misure minime di sicurezza

- definite negli art. 33, 34, disciplinare tecnico
- riguardano tutti i dati personali
- comprendono misure più stringenti in caso di
  - ✓ dati sensibili
  - ✓ dati giudiziari
- devono essere descritte nel documento programmatico sulla sicurezza

csiaf

Sicurezza informatica

Misure idonee di sicurezza

- sono riferite nell’art. 31
- non sono definite
- è cura del titolare o dei responsabili di definirle autonomamente e opportunamente
- devono essere costantemente aggiornate, indipendentemente dalle misure minime

csiaf

Sicurezza informatica

Documento Programmatico sulla Sicurezza (DPS)

è un manuale scritto contenente un piano per la sicurezza, che prova formalmente come vengono attuate le misure; descrive:

- situazione attuale
  - ✓ analisi dei rischi
  - ✓ distribuzione dei compiti
  - ✓ contromisure di sicurezza
  - ✓ distribuzione di responsabilità
- percorso di adeguamento

csiaf

Sicurezza informatica

Analisi del rischio

- Prevista nel disciplinare tecnico
- Deve essere presente nel DPS
- Consiste nella valutazione sistematica di
  - ✓ Danni derivanti dagli incidenti di sicurezza
  - ✓ Reale probabilità che gli incidenti si verifichino
- Permette di
  - ✓ Trovare un equilibrio fra costi e benefici per ridurre il rischio
  - ✓ Individuare i requisiti di sicurezza dell'organizzazione
- Analizza minacce, vulnerabilità, impatto degli incidenti per determinare il rischio di sicurezza (*possibilità che una minaccia si avvantaggi delle vulnerabilità per provocare un incidente*)

csiaf

Sicurezza informatica

- Per l'analisi e la gestione del rischio possono essere adottate metodologie dettagliate o semplificate, qualitative o quantitative
- Possono essere utilizzati approcci orientati ai processi o ai beni
- L'analisi può essere eseguita utilizzando appositi tool

csiaf

DPS CSIAF

DPS dello CSIAF:

- riguarda tutti i dati ‘detenuti’ dallo CSIAF
- contiene l’elenco dei trattamenti:
  - ✓ i trattamenti sono associati ai servizi erogati
  - ✓ i trattamenti sono suddivisi in:
    - ❑ trattamenti informatici (coinvolgono persone di altre strutture)
    - ❑ trattamenti cartacei

csiaf

DPS CSIAF

Responsabile: Dirigente

Responsabili (nominati dal Dirigente):

- afferenti allo CSIAF: responsabili di ufficio; ciascuno è responsabile relativamente ai servizi in carico all'ufficio
- esterni allo CSIAF: persone designate di concerto con il Dirigente di area o il Responsabile di struttura;

  sono designate per i trattamenti che coinvolgono altre strutture

csiaf

DPS CSIAF

Incaricati

(nominati da un responsabile o dal titolare):

- afferenti allo CSIAF:
  - ✓ “Incaricati per documentata preposizione”
  - ✓ “Incaricati speciali” (nominati dal Dirigente CSIAF)
- esterni allo CSIAF:
  - ✓ “Incaricati per documentata preposizione” (per tutto l’Ateneo o per la struttura)
  - Incaricati (nominati dal Responsabile della struttura o dal Dirigente CSIAF)

csiaf

DPS CSIAF

- Incaricati esterni allo CSIAF per documentata preposizione:
  - il personale di una struttura dell'Ateneo per il quale sia stata fatta una individuazione scritta degli ambiti del trattamento
- Incaricati esterni allo CSIAF:
  - il personale che per l'espletamento delle proprie funzioni deve trattare i dati

csiaf

DPS CSIAF

Incaricati:

Nello svolgimento dei compiti è fatto assoluto divieto agli Incaricati di comunicare e divulgare qualsivoglia dato personale. Tale obbligo di riservatezza si intende esteso anche al periodo successivo alla scadenza dell'incarico, fino a quando le suddette informazioni non vengano divulgate ad opera del Titolare, oppure divengano di dominio pubblico.

csiaf

Documento prescrittivo

Documento prescrittivo

- allegato del Documento Programmatico sulla Sicurezza (DPS) dello CSIAF
- contiene le regole comportamentali per la protezione dei dati, che costituiscono:
  - ✓ prescrizioni obbligatorie per gli incaricati che trattano dati CSIAF,
  - ✓ norme di accesso per tutti gli utenti della rete di Ateneo.

csiaf

Documento prescrittivo

Le regole comportamentali relative all'utilizzo delle apparecchiature di lavoro valgono per:

- stazioni di lavoro personali nel luogo di lavoro,
- stazioni di lavoro comuni a più persone, nel luogo di lavoro,
- stazioni di lavoro portatili,
- stazioni di lavoro dalle quali ci si connette in modalità remota,
- stampanti.

csiaf

Documento prescrittivo

Gestione degli accessi

- accesso dell'utente ai dati tramite credenziali di autenticazione (ed eventuali profili di autorizzazione):
  - ✓ identificativo (User ID), che è la parte pubblica,
  - ✓ parola chiave (password), che è la parte riservata.
- scelta della password robusta e difficilmente intuibile
- cautele per la segretezza della password
- obblighi relativi alla modifica della password

csiaf

Documento prescrittivo

Gestione della stazione di lavoro

- controllo durante le sessioni di trattamento dei dati
  - ✓ macchina incustodita
  - ✓ disconnessione
- protezione stazioni di lavoro:
  - ✓ password
  - ✓ screen saver
  - ✓ arresto sistema
  - ✓ backup su server o su CD

csiaf

Documento prescrittivo

Condivisione di dati

la condivisione dei dati sulle stazioni di lavoro personali

- deve essere ristretta alle sole persone incaricate di trattare tali dati
- deve essere conforme alle norme di sicurezza

per la condivisione di dati personali si raccomanda l'utilizzo di file server opportunamente gestiti secondo le norme di sicurezza previste;

csiaf

Documento prescrittivo

Prevenzione dai virus informatici

- installare il software antivirus in dotazione;
- configurare la protezione permanente e l'aggiornamento automatico via rete;
- verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine;
- fare attenzione a programmi e file scaricati o immessi.

N.B. tra un aggiornamento del programma antivirus ed il successivo è presente una finestra temporale di rischio di introdurre virus non ancora noti dal programma antivirus stesso

csiaf

Documento prescrittivo

Aggiornamenti software

Per prevenire, sulla propria stazione di lavoro, accessi non autorizzati che violino il sistema e compromettano la sua integrità è necessario seguire una politica di aggiornamento dei software presenti sulla stazione di lavoro in modo da introdurre regolarmente le modifiche o le nuove versioni emesse per proteggere i sistemi:

- configurare, ove possibile, l'esecuzione automatica degli aggiornamenti del sistema operativo, ovvero
- configurare, ove possibile, lo scaricamento automatico dalla rete degli aggiornamenti (patch) del sistema operativo ed eseguire l'installazione non appena disponibile;

csiaf

Documento prescrittivo

Materiale ottenuto come output da apparecchiature informatiche e non:

- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine

csiaf

Accesso a INTERNET

La Rete di Ateneo è connessa, e dunque sua parte integrante, alla Rete del GARR (Gestione Ampliamento Rete Ricerca)

La Rete del GARR è la rete della Comunità Italiana delle Università e della Ricerca Scientifica e Tecnologica

In base alla "Acceptable Use Policy (AUP) della rete GARR", l'utilizzo è consentito esclusivamente per attività istituzionali, cioè "la attività di ricerca, la didattica, le funzioni amministrative"

csiaf

Accesso a INTERNET

Non sono ammesse sulla rete azioni

- contrarie alla legislazione
- contrarie alle Norme di Internet (Netiquette)

L'utilizzo non corretto della rete può avere conseguenze, a seconda dei casi:

- sul referente della stazione di lavoro dalla quale è stata fatta l'infrazione;
- sui referenti della rete dell'Università di Firenze;
- sui referenti del dominio unifi.it

csiaf

Accesso a INTERNET

Servizi di sicurezza CERT

- del GARR (GARR-CERT),
- dell'Università (CERT-UNIFI).

Il servizio CERT-UNIFI opera in base a protocolli definiti per la gestione di incidenti ed abusi verificatisi nella Rete di Ateneo

csiaf

Accesso a INTERNET

Posta elettronica

L'utilizzo della posta elettronica è regolamentato dal

Regolamento di utilizzo dei servizi di comunicazione

- ✓ viene assegnato un indirizzo e-mail a tutto il personale
- ✓ vengono assegnati indirizzi di funzione a tutte le figure istituzionali
- ✓ vengono definite mailing list di Ateneo per le comunicazioni attinenti alle attività istituzionali

csiaf

Accesso a INTERNET

Viene fatto espresso divieto di:

- utilizzare per le comunicazioni inerenti le attività istituzionali caselle di posta diverse da quelle del dominio *unifi.it;*
- inviare lettere a catena ovvero messaggi ripetuti;
- diffondere notizie non veritiere e non verificate;
- inondare di messaggi indesiderati (spamming);
- non rispettare le normative sulla proprietà intellettuale;
- diffondere consapevolmente virus.

Devono essere seguite le norme di comportamento presenti nell'allegato del Regolamento

csiaf

Sicurezza dei sistemi informatici

FINE

BUON LAVORO!

csiaf