ALL (4)

MINISTERO DELLA GIUSTIZIA

Tribunale di Caltanissetta

Documento programmatico
Della sicurezza

Caltanissetta, 31marzo 2012

RIFERIMENTI

- Circolare Direzione Generale dell'Organizzazione Giudiziaria del 21/12/2000, in materia di "Misure minime di sicurezza per il trattamento dei dati"
- Decreto Ministeriale 24/05/2001 "Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia" (*pubblicato sulla G.U. n. 128 del 05/06/2001)*
- Linee guida per lo sviluppo di piani di sicurezza dei sistemi informatici del Ministero della Giustizia (versione 1.5 del 12/11/2002) del Gruppo di Sicurezza del Politecnico di Torino, redatte sotto contratto con la Direzione Generale Sistemi Informativi Automatizzati (DGSIA)
- Decreto Legislativo 30/06/03, n. 196 "Codice in materia di protezione dei dati personali" (*pubblicato sulla G.U. n. 174 del 29/07/2003 – suppl. ord. 123/L*)

1. INQUADRAMENTO GENERALE ED ATTI PRELIMINARI

1.1 Che cosa è, a cosa e a chi serve il presente documento programmatico della sicurezza

Il presente documento rappresenta il documento programmatico della sicurezza di questo Ufficio relativamente al sistema informatico e deriva sia da precisi obblighi di legge (DPR 318/99, DM 24/05/2001, D.Lvo 30/06/03, n. 196, di seguito "codice") che dalla complessità del sistema informatico degli Uffici Giudiziari. Infatti, quanto più un sistema è complesso, tanto maggiore è l'esigenza di procedere alla redazione di un piano di sicurezza in modo *formale* e *sistematico*, per evitare di trascurare o sottovalutare qualche aspetto.
Nel presente documento viene considerato il sistema informativo dell'Ufficio, ossia l'insieme dei dati, delle procedure, dei sistemi di elaborazione e telecomunicazione e delle persone che trattano le informazioni vitali per il funzionamento dell'Ufficio stesso. In particolare ci si è ristretti a considerarne più specificamente gli aspetti di sicurezza informatica, ossia tutti gli aspetti inerenti attacchi e quindi misure di protezione di tipo informatico. Talvolta si è espanso un po' questo campo di azione, considerando anche aspetti *logistici* (quali la protezione dei locali ove sono collocati i server dell'Ufficio) ed *organizzativi* (come il divieto di comunicare la propria password ad estranei), perché è praticamente impossibile proteggere un sistema informatico con misure puramente di tipo informatico, ossia senza considerare almeno alcuni aspetti relativi alla collocazione del sistema ed alla sua modalità d'uso da parte del personale autorizzato.
Per la stesura del presente Documento Programmatico della Sicurezza (in breve DPS) ci si è basati sulla normativa riportata nei riferimenti. Il DPS è adottato dagli Uffici Giudiziari entro il 31 marzo di ogni anno ed è diretto a tutto il personale dell'Ufficio.

1.2 Individuazione delle figure di riferimento e definizioni

Secondo l'art. 3 del D.M. 24/05/2001, e l'art. 19 Allegato B al codice, "il Dirigente Amministrativo dell'ufficio è il responsabile della tenuta dei registri e provvede alla stesura del piano della sicurezza di cui al successivo art. 7, secondo le indicazioni della Direzione Generale per i sistemi informativi automatizzati (di seguito DGSIA), vigilando sulla sua applicazione".
L'art. 7 c.6 del D.M. 24/05/2001 recita: "La vigilanza sulla predisposizione e sull'applicazione dei piani di sicurezza è esercitata dai capi degli uffici, secondo le rispettive competenze, avvalendosi anche di un esperto informatico designato dalla DGSIA".
L'art. 2 del D.M. del 24/05/2001 stabilisce che "Il sistema informativo dell'ufficio soddisfa le seguenti proprietà: a) disponibilità, b) integrità, c) autenticità, d) controllo degli accessi".
A questi si aggiunge il criterio della riservatezza, introdotto dall'art. 3 del "codice".
L'art. 4 del D.M. del 24/05/2001 prevede inoltre che "...L'Amministratore di Sistema, ora **Amministratore Dei Servizi Informatici (ADSI),** assicura la conduzione operativa del sistema informativo, effettuando tutte le operazioni necessarie a garantire le proprietà di cui all'art. 2."
Per quanto concerne le figure che intervengono nell'ambito del piano della sicurezza e del trattamento dei dati si richiama l'art. 4 del codice:
- capoverso f si intende "per titolare la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza":
- capoverso g si intende "per responsabile la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".
Con riferimento alle figure designate, il codice all'art. 29 dispone:

"1. Il **responsabile** è designato dal titolare facoltativamente.

2. 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, ivi compreso il profilo relativo alla sicurezza"...

5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni".
Profili di responsabilità:
Il titolare deve individuare e adottare preventivamente all'effettivo trattamento dei dati le misure di sicurezza minime previste dalla legge (articolo 33).
Se le misure di sicurezza adottate non rispettano i parametri minimi, non sono "idonee" e, di conseguenza, scatta la responsabilità penale in capo a chi abbia omesso di adottarle. Le sanzioni previste sono l'arresto sino a due anni o l'ammenda da diecimila a cinquantamila euro.
La sola individuazione di misure di sicurezza che rispettino i parametri previsti dalla legge non è sufficiente a liberare da ogni responsabilità il soggetto che effettua il trattamento. Se le misure adottate, pur in linea con quanto previsto riguardo alle misure minime, non si rivelano in concreto idonee ad evitare il danno, vi è comunque attribuzione della responsabilità civile ex articolo 2050 codice civile.

1.3 Il Titolare del trattamento

Ai sensi dell'art. 46 del "codice", "gli Uffici giudiziari di ogni ordine e grado sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento".
Il soggetto responsabile di tale funzione viene individuato nel Magistrato Dirigente dell'Ufficio, ai sensi del citato art. 28 del "codice"; già in relazione al previgente quadro normativo, la Direzione Generale dell'Organizzazione Giudiziaria aveva ricondotto al Magistrato Dirigente il Titolare del trattamento dei dati[1] .
Rispetto al "DPS", il Magistrato Dirigente ha compiti di vigilanza sulla predisposizione e sull'applicazione dei piani della sicurezza (artt. 7 co. 6 D.M. 245/2001 e 29 co. 5 "codice").
Pertanto il titolare del trattamento è il Presidente del Tribunale dott. Claudio dall'Acqua.

1.4 Il Responsabile del trattamento

La designazione del responsabile del trattamento è facoltativa. In mancanza, le responsabilità rimangono in capo al titolare.
Ove il Magistrato Dirigente ritenga di procedere ad individuare il responsabile del trattamento, avrà piena discrezionalità nella scelta.
Tuttavia, in considerazione sia del precedente assetto organizzativo in materia di protezione dei dati personali, che individuava nel Dirigente Amministrativo il Responsabile del trattamento, sia in relazione alle generali competenze e responsabilità attribuite al Dirigente Amministrativo dalla normativa sulla dirigenza e da quella sulla gestione dei registri informatizzati, si rappresenta l'opportunità di fare riferimento al Dirigente Amministrativo dell'ufficio per l'investitura della responsabilità nel trattamento dei dati, ferma l'autonomia del Magistrato Dirigente.
L'art. 29 prevede, infatti, che tale figura sia scelta tra i "soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" e, a tale specifico proposito, il dirigente amministrativo è anche qualificato quale *responsabile della tenuta dei registri informatizzati* dall'art. 3 D.M. 24/5/2001[2].
Il Responsabile del trattamento, in accordo con il C.I.S.I.A., in particolare:

- provvede alla stesura e all'aggiornamento entro il 31 marzo di ogni anno del piano di sicurezza del sistema informativo dell'ufficio, con la collaborazione dell'Amministratore Dei Servizi Informatici, secondo gli standard definiti dalla DGSIA vigilando sulla sua applicazione;
- adotta (art. 31 "codice"), riguardo al trattamento di dati personali, le misure minime di sicurezza (art. 33 "codice") con le modalità previste dal Titolo V della Parte I, Capo II del "codice" e dal disciplinare tecnico contenuto nell'Allegato B al "codice" stesso.
- verifica l'adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali all'aggiornamento periodico del disciplinare tecnico predisposto dal Ministro della Giustizia di concerto con il Ministro per l'Innovazione e le Tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore (art. 36 del "codice");
- decide, varia ed approva la lista degli utenti abilitati e i relativi livelli di abilitazione;
- decide e approva la dislocazione fisica delle attrezzature informatiche, sentito l'ADSI.

[1] Circolare D.G.O.G. 21/12/2000, in materia di "Misure minime di sicurezza per il trattamento dei dati".
[2] Anche nel precedente quadro normativo, il dirigente amministrativo era stato individuato quale responsabile del trattamento dei dati: "Il responsabile del trattamento ha principalmente un ruolo di coordinamento: impartire disposizioni agli incaricati, agli amministratori di sistema e ai preposti alle parole chiave, riportare al Capo dell'ufficio le problematiche di maggior rilievo per una decisione in merito, assicurarsi che le disposizioni emanate siano osservate, e così via. Si tratta quindi di una figura interna all'ufficio, con un ruolo dirigenziale: nel caso degli uffici giudiziari, ad esempio, risulta abbastanza naturale l'individuazione del responsabile nel Dirigente preposto alla cancelleria o segreteria". Circolare D.G.O.G. citata

Viene designato responsabile del trattamento il Dirigente Amministrativo del Tribunale dott. Michele Testaquatra.

1.5 Incaricati del trattamento

Gli incaricati del trattamento, secondo l'art. 30 del "codice", sono i soggetti abilitati ad operare sui dati, sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni ricevute.
"La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima" (art. 30 co. 2 del "codice").
Tra gli incaricati è opportuno evidenziare una specifica e settoriale responsabilità in capo ai "funzionari" (o equiparati) titolari delle aree organizzative o dei singoli servizi giudiziari, che per comodità di seguito saranno indicati quali *Responsabili amministrativi.*

In particolare, con riferimento al trattamento dei dati, i *Responsabili amministrativi* devono farsi carico delle seguenti incombenze:
- proporre al *Responsabile del trattamento* il nominativo degli incaricati da accreditare, di coloro che devono essere disabilitati ed eventuali modifiche da apportare al profilo utente, in coerenza con le politiche di governo dell'ufficio;
- rilevare i fabbisogni informatici di area;
- curare il corretto utilizzo degli applicativi installati nella propria area, da parte degli incaricati/utenti, con particolare riferimento alla qualità dei dati inseriti nelle basi di dati;
- collaborare con l'Amministratore Dei Servizi Informatici, segnalando eventuali anomalie nella tenuta dei sistemi informativi;

1.6 Amministratore Dei Servizi Informatici

I compiti dell'Amministratore Dei Servizi Informatici (AdSI) sono svolti da una o più figure professionali del settore informatico a seconda delle dimensioni dell'ufficio e del numero degli edifici. Un unico soggetto può svolgere tali funzioni per più uffici o per più edifici.
Nel caso siano stati individuati più soggetti per lo svolgimento delle funzioni di amministratore Dei Servizi Informatici, la DGSIA designa il coordinatore (art. 4, c.5 DM 24/05/01).
Al fine di coprire con continuità il servizio, il CISIA distrettuale provvederà caso per caso, e mediante comunicazione scritta agli Uffici interessati, ad individuare dei sostituiti degli AdSI assegnati agli Uffici stessi, sulla base della corrente disponibilità delle risorse di personale.
L'Amministratore Dei Servizi Informatici:
- viene nominato dalla D.G.S.I.A. ed è individuato tra gli esperti informatici del C.I.S.I.A. competente per territorio (art. 4 co. 4 DM 24/5/2001);

L'Amministratore Dei Servizi Informatici relaziona al *Responsabile del trattamento* e altresì al C.I.S.I.A. per i casi che coinvolgano la sicurezza della Rete Unica della Giustizia (nel seguito RUG), sugli eventi e i comportamenti in difformità o in violazione del presente Piano o della normativa sulla sicurezza nella gestione del sistema informativo.
Per lo svolgimento di suddetti compiti, l'Amministratore Dei Servizi Informatici si avvale della collaborazione del personale del Servizio Assistenza Tecnica assegnato alle sedi giudiziarie con nota del Cisia Palermo 17028 del 24.06.2010, in particolare per;
- la redazione ed il controllo dei registri e dei cataloghi, utilizzando opportuni strumenti *software* ausiliari individuati dal C.I.S.I.A., che rendano la redazione e il mantenimento un processo automatico sostenibile;

- la stesura dell'inventario delle risorse hardware e software.

2. REGISTRO DELLE RISORSE UMANE

Nel presente DPS sono elencate le informazioni anagrafiche ed organizzative relative al personale, specificando a quali aree può accedere e quali apparecchiature può utilizzare. Per ogni stazione di lavoro è riportato l'elenco del software installato sviluppato specificatamente per l'informatizzazione degli uffici e il software di mercato.
(Allegato1-Registro delle risorse umane)

- Secondo quanto previsto dall'art. 1 DM 24/5/2001, è necessario disporre di un quadro completo delle risorse umane, ovvero del personale interno all'ufficio e personale esterno autorizzato all'accesso ai dati e ai trattamenti (ad es. ufficiali di PG, personale Servizio Assistenza Tecnica, ecc...), nonché dei servizi di interoperabilità a ciascun soggetto associati.
-
- 2.1 Risorse umane

E' importante che qualsiasi modifica relativa alle risorse umane venga comunicata, per evitare il rischio di avere soggetti non inventariati, secondo la seguente procedura:

- gli uffici coinvolti dalle modifiche delle risorse umane devono darne comunicazione al *Responsabile del trattamento* o ad un referente da questi incaricato, il quale comunica la variazione (anche di tipo hardware e software) all'Amministratore Dei Servizi Informatici.

Le possibili figure coinvolte sono:

- *Responsabile del trattamento* o referente incaricato (preventivamente comunicato all'Amministratore Dei Servizi Informatici);
- Amministratori Dei Servizi Informatici (coordinano e partecipano alla gestione del sistema informatico, avvalendosi della collaborazione dei tecnici del Servizio Assistenza Tecnica);
- Tecnici esterni del Servizio Assistenza Tecnica ,su segnalazione dell'Amministratore Dei Servizi Informatici, eseguono le modifiche del caso.

Le unità organizzative degli Uffici che possono essere coinvolte sono:

- Ufficio del Personale (nel caso di assegnazione del dipendente ad altro servizio, nuova nomina, destituzione, fine servizio: comunica l'evento al Responsabile);
- Ufficio del Consegnatario economo (dismissione del bene per obsolescenza, per danni gravi, acquisizione di nuove apparecchiature: comunica l'evento al Responsabile);
- Cancelleria/segreteria della specifica area di lavoro.
-
- Questa Procura Generale, giusta nota del Direttore Generale SIA del 12/08/2009, ID. n. 23258/09, ha provveduto in data 25/08/2009 a nominare quale responsabile del trattamento dati il dr. Stefano Gigli relativamente alla conduzione sistemistica di server e postazioni lavoro ed in particolare alla gestione dei log di accesso del personale esterno.
- Per quanto riguarda il trattamento dei dati di questa Corte d'Appello, il responsabile sarà il Dirigente Amministrativo.

2.2 Software

E' possibile installare ed utilizzare esclusivamente *software* appartenente ad una delle tre seguenti categorie (art. 12 c. 1 DM 24/5/2001):

- *software* commerciale: solo se munito di idonea licenza d'uso ovvero se fornito nell'ambito di accordi quadro nazionali dalla D.G.S.I.A.;
- applicativi di rilevanza nazionale; rilasciati dalla D.G.S.I.A., che ne certifica la conformità ai sensi art. 3 DM 264/2000; nessuna modifica o personalizzazione di tali applicativi è consentita da parte di soggetti diversi dalla D.G.S.I.A. (art. 18 co. 3 DM 24/5/2001);
- applicativi realizzati a livello locale, purchè conformi alle regole tecniche e alle regole tecnico procedurali (decreti 264/2000 e 24/5/2001) e soltanto se autorizzati dal Capo dell'ufficio.

Inoltre sulle postazioni non vengono installati sofware che non risultino utili alle attività degli utenti, sia per non appesantire l'elaboratore, sia per evitare eventuali conflittualità con altri software necessari.

- La totalità degli applicativi specifici in uso presso l'Ufficio della Corte d'Appello sono di emanazione ministeriale e pertanto regolarmente forniti da parte dei superiori Uffici. In particolare gli applicativi utilizzati sono i seguenti: **Applicativo per accesso al DAP, SIEP, GECO, PROTEUS, SIAMM, SICOGE, SIPERT, Applicativo per accesso al Casellario, Rete Ponente, SICC, SIL o SICID, Re.Ca.**
-

3. MISURE DI SICUREZZA

3.1 Protezione fisica delle aree e dei locali

In linea con il DM 24/5/2001, capo III, e ai sensi dell'art. 19.4 all. B del "codice", è necessario adottare un piano di protezione fisica delle aree e dei locali in cui sono presenti quelle parti del sistema informativo che gestiscono i registri informatizzati. Si rimanda inoltre alle prescrizioni del responsabile per la sicurezza dei lavoratori ai sensi della L. 626/94 e del responsabile antincendio ai sensi della L. 818/84. Tali responsabili sono nominati dai singoli uffici secondo le normative sopra citate.

3.2 Accesso alle Sale Server

L'accesso alle sale *server* ed ai locali tecnici è consentito solo alle persone autorizzate dal *Responsabile del trattamento*, o da soggetto da questo delegato, Incaricato amministrati o dall'Amministratore Dei Servizi Informatici (art. 11 c. 2 DM 24/5/2001).

Il soggetto che facendo richiesta all'Ufficio sarà autorizzato all'accesso alla sala server dovrà essere accompagnato e assistito nelle operazioni dai tecnici del Servizio di Assistenza Tecnica o dall'Amministratore Dei Sevizi Informatici.

Per la gestione delle aree comuni (quali le sale server, gli armadi di piano etc.) saranno concordate dagli stessi Uffici interessati le linee guida comuni, la cui redazione sarà definita tra i Responsabili del Trattamento con il supporto tecnico dell'Amministratore Dei Servizi Informatici competente per le aree comuni.

Il Server virtuale della Corte d'Appello è distinto in: CAPP_AMM (per SIPERT), SVCEDCLUTE004 su ADN (per RE.CA. e cartelle condivise). Il SICID, è ospitato presso le sale server di Messina.

3.3 Custodia delle chiavi di accesso delle sale server e dei locali relativi agli apparati di rete

Tutte le chiavi relative ai locali della sala server, dei locali ove sono ubicati gli apparati di rete, nonché degli armadi di rete stessi dovranno essere custoditi dal Responsabile del Sistema Informativo o da un suo delegato. Verrà consegnata una copia della chiave al personale del Servizio di Assistenza Tecnica e/o agli AdSI, per velocizzare e agevolare gli accessi ai server nel caso di guasti e per la manutenzione ordinaria. Qualora la porta della sala *server* sia dotata di badge, l'accesso mediante chiavi deve avvenire solo in situazioni di emergenza (per esempio, temporaneo malfunzionamento del meccanismo *hardware* o *software* di controllo della porta elettrificata).
In conformità alle linee guida per le procedure di sicurezza dei sistemi informativi ed automatizzati emanate dal C.I.S.I.A. di Palermo e redatte sulla base del Decreto Ministeriale del 5 maggio 2001 in merito alle regole procedurali per la tenuta dei registri informativi automatizzati e tenendo altresì conto delle indicazioni di carattere generale contenute nel documento del C.N.P.A. circa la definizione del piano per la sicurezza dei sistemi informativi automatizzati della Pubblica Amministrazione, si rinnova la proposta di Attivazione di un sistema di rilevazione automatica degli ingressi alle Sale Server, tramite lettore di badge, così da gestire in maniera informatizzata il "Registro di sicurezza degli accessi"

3.4 Norme di comportamento per gli utenti

Anche le migliori e più sofisticate misure di sicurezza possono essere vanificate da un comportamento non appropriato degli utenti del sistema in oggetto. E' perciò molto importante fornire agli utenti un codice di comportamento che li aiuti nel partecipare alla costruzione di un sistema sicuro.
Nell'allegato Manuale di sicurezza per gli utenti e nelle Linee guida sull'uso delle password vengono elencati i principali suggerimenti da fornire ad un utente per aumentare la sicurezza globale del sistema. E' opportuno che tali norme di comportamento siano distribuite ad ogni nuovo utente del sistema e siano consultabili via rete. Ad ogni aggiornamento delle suddette norme è importante segnalare agli utenti la disponibilità della nuova versione, evidenziando che cosa è cambiato rispetto alla versione già in loro possesso. Ad ogni utente deve essere associato un profilo in base al ruolo che ricopre nell'ufficio. I profili degli utenti e la gestione delle password sono effettuate a livello nazionale attraverso il sistema di Active Directory Nazionale (ADN)

4. SICUREZZA DELLE RETI

La prima linea di difesa di qualunque sistema informatico è la protezione dell'infrastruttura di rete. A questo riguardo vengono qui considerati i principali pericoli che si corrono ed elencate le contromisure da adottare.

4.1 Modem

La disponibilità di modem sulle postazioni di lavoro costituisce una potenziale minaccia perché il loro uso per instaurare un collegamento con una rete esterna potrebbe sottoporre la rete ad attacchi che aggirano i firewall ed eludono i sistemi di monitoraggio e di controllo.

Il regolamento informatico del Ministero vieta espressamente l'uso dei (art. 23 comma 5 del DM 24/05/2001: "L'utente è tenuto a non utilizzare, su postazioni di lavoro collegate alla rete locale dell'ufficio, *modem* o altri strumenti di connessione con l'esterno").
Tale norma deve essere rigorosamente osservata, poiché un *modem* è facilmente installabile e configurabile, ove si disponga degli opportuni privilegi, ed è spesso incluso nei computer portatili.

Sarebbe opportuno prevedere l'eventuale segnalazione automatica al Responsabile del singolo Ufficio in caso di telefonate a numeri noti di Internet Service Provider esterni.
Nel caso in cui sia strettamente necessario l'utilizzo di modem su alcune postazioni di lavoro, sarà cura dell'utente farne richiesta scritta e motivata al Responsabile del Trattamento dell'Ufficio, il quale autorizzerà per iscritto l'utente all'uso del modem.
In questo caso l'utente deve seguire le norme suggerite nell'allegato Manuale di sicurezza per gli utenti (disconnessione dalla rete locale durante il periodo di attivazione del modem, installazione locale di un antivirus aggiornato, installazione di un Personal Firewall con configurazione molto restrittiva). In ogni caso l'utente diventa responsabile di eventuali danni che possono derivare ai sistemi informatici da un uso non appropriato del modem.
E' comunque consigliabile ed opportuno, in caso di necessità imprescindibile di utilizzo di *modem*, individuare dei *computer* dedicati da tenere debitamente scollegati dalla LAN interna (cd. postazioni *stand-alone*).
non è assolutamente consentita l'installazione di *modem* utilizzabili da ditte esterne per l'amministrazione remota dei sistemi in uso agli uffici.

4.2 Connessioni esterne

Nel caso che un collegamento diretto dall'Ufficio ad una rete esterna sia considerato assolutamente indispensabile, l'esistenza di tale collegamento deve essere adeguatamente motivata e segnalata alla DGSIA affinché sia autorizzato e catalogato tra i punti di pericolo della rete del Ministero dal Centro Gestione Firewall, che provvederà ad attuare le conseguenti policy di sicurezza.
Il collegamento deve essere tempestivamente dismesso o anche solo temporaneamente disattivato qualora vengano a mancare le motivazioni per cui è stato creato.
Il collegamento non può essere attestato direttamente all'interno della rete locale ma deve essere posizionato all'esterno del firewall di sede in modo che la sua sicurezza sia gestita in modo centralizzato dal Centro Gestione Firewall del Ministero.
Se il collegamento non è di tipo aperto ma è equiparabile ad una connessione punto-punto con un singolo ente esterno, allora deve essere protetto tramite tecniche di autenticazione e cifratura secondo lo standard IPsec.

4.3 PC Portatili

Nel caso di utilizzo da parte degli utenti dei computer portatili, si precisa che dovranno essere rispettati i seguenti vincoli.
Dovrà essere installato sul computer l'antivirus in utilizzo dall'Amministrazione (attualmente McAfee Virus Scan). I file di definizione virus dovranno essere aggiornati con cadenza periodica.
Dovrà essere installato e opportunamente configurato su ogni computer un software firewall, in modo tale da rendere più sicuro il collegamento in caso di connessioni ad internet dall'esterno della rete giustizia (i.e. in caso di collegamenti tramite Internet Provider pubblici). Tale compito verrà svolto dai tecnici del Servizio di Assistenza Tecnica.

4.4 Virus e misure antivirus

Per garantire un'adeguata protezione l'aggiornamento dell'antivirus avviene direttamente dal Server di Dominio Nazionale. L'ADSI
deve verificare che siano effettuate dal servizio di Assistenza tecnica Unificata, le seguenti attività:

- informare gli utenti dei comportamenti a rischio secondo quanto indicato nelle "Linee guida per la sicurezza dell'informazione" redatto dalla DGSIA:
-

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato;
- evitare di utilizzare giochi o software peer to peer (software che permettono la condivisione di files sulla rete i.e. Imesh, Gnutella, audiogalaxy, Napster software per le chat ICQ e simili);
- assicurarsi di non accendere al proprio computer con unità esterne di memoria rimovibili inserite. Infatti se queste fossero infette, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file. Per limitare i rischi connessi a questo comportamento in fase di installazione delle postazioni di lavoro è possibile impostare il BIOS in modo da avere come "primary boot device" il disco rigido di avvio e proteggere l'accesso al BIOS tramite password;
- proteggere i dischetti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- salvare o sottoporre a back-up i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:

- diffondere messaggi e-mail di provenienza dubbia o partecipare a "catene di S. Antonio" e simili, che possono generare traffico inutile (veri scopi di chi diffonde queste mail).
- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione antivirus;
- visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come richiamo per attirare visitatori su cui condurre attacchi informatici;
- modificare la configurazione del software antivirus.

Per ulteriori dettagli si rinvia al Manuale di sicurezza dell'utente.

5. INTEGRITÀ E DISPONIBILITÀ DEI DATI

A causa di guasti accidentali delle apparecchiature informatiche, dovuti a variabili esterne o dolose (sbalzi di tensione, incendi, attacchi deliberati, etc.), il rischio di perdita dei dati può essere notevole.
L'art. 10 del DM 24/5/2001 prescrive per ciascun ufficio idonee politiche e procedure per il salvataggio (backup) e per il recupero (recovery) dei dati, sia a livello di sistema sia a livello di database management system.

5.1 Back-up and Restore

I dati da sottoporre a salvataggio o *back up* sono classificati in **dati di sistema** (necessari per il corretto funzionamento del sistema operativo, del *software* di base, del *database* management system, delle applicazioni installate, etc.) e **dati utente** (documenti, fogli elettronici, archivi di posta elettronica, ecc.).
Con riferimento all'art. 10 del DM 24/5/2001 commi 2, 3 e 4, si adottano le seguenti politiche di *back up*:
I dati presenti sui server ed i dati sensibili devono essere sottoposti a back-up completo con frequenza settimanale.
I back up dei nuovi dati o dei dati modificati devono essere effettuati con frequenza giornaliera, in maniera incrementale laddove possibile, altrimenti in maniera completa. E' possibile approntare anche un sistema giornaliero di back up incrociato fra i server, in aggiunta o in alternativa a quello su supporto rimovibile.
I file di log devono essere trattati come dati sensibili e quindi salvati periodicamente.
Per ogni supporto di back-up il costruttore specifica un numero massimo di operazioni di scrittura. Per evitare che un back-up risulti illeggibile, si raccomanda di non riutilizzare i supporti di back-up che sono stati riscritti un numero di volte pari al 95% di quanto raccomandato dal produttore.
Appena terminate le operazioni, i supporti di back-up devono essere riposti negli armadi di sicurezza, blindati ed ignifughi, collocati all'esterno delle sale server, nelle apposite sale di conservazione dei back-up, al fine di evitare accessi non autorizzati e trattamenti non consentiti . Tali armadi devono sempre essere mantenuti chiusi a chiave.
I supporti rimovibili contenenti dati sensibili o comunque essere resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
A richiesta dell'utente e compatibilmente con le esigenze di spazio sul server, per il back-up dei dati degli utenti sono messe a disposizione degli stessi, delle aree sui server dove gli utenti possono salvare i dati di cui desiderano sia fatto il back-up. La configurazione di ciascuna quota è tale da consentire l'accesso in lettura e scrittura solo ed esclusivamente all'utente proprietario e l'accesso in sola lettura all'Amministratore di sistema. E' cura di ciascun utente provvedere a copiare sulla propria quota i file che desidera sottoporre a *back up*.

6. CONTINUITÀ DEGLI APPLICATIVI

Una prima misura indispensabile per tutti i server è di essere dotati di un gruppo di continuità (articolo 11 comma 3 DM 24/5/2001) per garantirne il funzionamento per un breve periodo anche in mancanza di alimentazione elettrica di rete. E' bene che il gruppo di continuità sia collegato al server in modo che se l'alimentazione di rete non viene ripristinata entro il tempo per cui il gruppo è dimensionato, allora venga effettuato automaticamente uno shutdown del sistema per evitare che possa danneggiarsi quando anche questo tipo di alimentazione venga a mancare.

7. RESPONSABILITA' ED AGGIORNAMENTO DEL PDS

Il documento programmatico della sicurezza viene aggiornato entro il 31 marzo di ogni anno, tenendo conto degli adeguamenti al disciplinare tecnico, apportati con decreto del Ministro della Giustizia di concerto con il Ministro per l'Innovazione e le Tecnologie, in relazione all'evoluzione tecnica e l'esperienza maturata nel settore.
All'interno del DPS, ogni qual volta venga identificata un'attività da svolgere, deve anche essere indicata a chi è attribuita la responsabilità dello svolgimento, identificando la persona non solo con nome e cognome ma tramite il ruolo o l'incarico ricoperto all'interno del Ministero. In questo modo, se una persona dovesse lasciare il Ministero o cambiare mansione, la responsabilità viene automaticamente attribuita alla persona che ne ha rilevato il ruolo.

IL RESPONSABILE DEL TRATTAMENTO DEI DATI

IL DIRIGENTE DEL TRIBUNALE

Dott. Michele Testaquatra

IL TITOLARE DEL TRATTAMENTO DEI DATI

IL PRESIDENTE DEL TRIBUNALE

Dott. Claudio Dall'Acqua

DISPOSIZIONI TEORICHE E PRATICHE IN MATERIA DI TUTELA E PROTEZIONE DEI DATI TRATTATI

1. RUOLI E PROFILI

Vengono illustrati i ruoli e profili di rilevanza in materia di tutela dei dati, previsti dal Codice della privacy adottato con DLvo 196/03

1.1 Titolare del trattamento

Ai sensi dell'art. 46 del "codice", "gli Uffici giudiziari di ogni ordine e grado sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento".
Il soggetto responsabile di tale funzione viene individuato nel Magistrato Dirigente dell'Ufficio, ai sensi del citato art. 28 del "codice"; già in relazione al previgente quadro normativo, la Direzione Generale dell'Organizzazione Giudiziaria aveva ricondotto al Magistrato Dirigente il Titolare del trattamento dei dati[1] .
Il Magistrato Dirigente ha compiti di vigilanza sulla predisposizione e sull'applicazione dei piani della sicurezza .
Pertanto il titolare del trattamento è il Presidente del Tribunale dott. Daniele Marraffa.

1.2 Il Responsabile del trattamento

La designazione del responsabile del trattamento è facoltativa. In mancanza, le responsabilità rimangono in capo al titolare.
Ove il Magistrato Dirigente ritenga di procedere ad individuare il responsabile del trattamento, avrà piena discrezionalità nella scelta.
Tuttavia, si rappresenta l'opportunità di fare riferimento al Dirigente Amministrativo dell'ufficio per l'investitura della responsabilità nel trattamento dei dati, ferma l'autonomia del Magistrato Dirigente.L'art. 29 prevede, infatti, che tale figura sia scelta tra i "soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" e, a tale specifico proposito, il dirigente amministrativo è anche qualificato quale *responsabile della tenuta dei registri informatizzati* dall'art. 3 D.M. 24/5/2001[2].
Il Responsabile del trattamento, in accordo con il C.I.S.I.A., in particolare:

- adotta (art. 31 "codice"), riguardo al trattamento di dati personali, le misure minime di sicurezza (art. 33 "codice") con le modalità previste dal Titolo V della Parte I, Capo II del "codice" e dal disciplinare tecnico contenuto nell'Allegato B al "codice" stesso.
- verifica l'adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali all'aggiornamento periodico del disciplinare tecnico predisposto dal Ministro della Giustizia di concerto con il Ministro per l'Innovazione e le Tecnologie, in

[1] Circolare D.G.O.G. 21/12/2000, in materia di "Misure minime di sicurezza per il trattamento dei dati".
[2] Anche nel precedente quadro normativo, il dirigente amministrativo era stato individuato quale responsabile del trattamento dei dati: "Il responsabile del trattamento ha principalmente un ruolo di coordinamento: impartire disposizioni agli incaricati, agli amministratori di sistema e ai preposti alle parole chiave, riportare al Capo dell'ufficio le problematiche di maggior rilievo per una decisione in merito, assicurarsi che le disposizioni emanate siano osservate, e così via. Si tratta quindi di una figura interna all'ufficio, con un ruolo dirigenziale: nel caso degli uffici giudiziari, ad esempio, risulta abbastanza naturale l'individuazione del responsabile nel Dirigente preposto alla cancelleria o segreteria.". Circolare D.G.O.G. citata.

relazione all'evoluzione tecnica e all'esperienza maturata nel settore (art. 36 del "codice");
- decide, varia ed approva la lista degli utenti abilitati e i relativi livelli di abilitazione;
- decide e approva la dislocazione fisica delle attrezzature informatiche, sentito l'ADSI.

Viene designato responsabile del trattamento il Dirigente Amministrativo del Tribunale la dott.ssa Rosanna Antonia Gallo.

1.3 Amministratore Dei Servizi Informatici

I compiti dell'Amministratore Dei Servizi Informatici (AdSI) sono svolti da una o più figure professionali del settore informatico a seconda delle dimensioni dell'ufficio e del numero degli edifici. Un unico soggetto può svolgere tali funzioni per più uffici o per più edifici.
Nel caso siano stati individuati più soggetti per lo svolgimento delle funzioni di amministratore Dei Servizi Informatici, la DGSIA designa il coordinatore (art. 4, c.5 DM 24/05/01).
Al fine di coprire con continuità il servizio, il CISIA distrettuale provvederà caso per caso, e mediante comunicazione scritta agli Uffici interessati, ad individuare dei sostituiti degli AdSI assegnati agli Uffici stessi, sulla base della corrente disponibilità delle risorse di personale.
L'Amministratore Dei Servizi Informatici:
- viene nominato dalla D.G.S.I.A. ed è individuato tra gli esperti informatici del C.I.S.I.A. competente per territorio (art. 4 co. 4 DM 24/5/2001);

L'Amministratore Dei Servizi Informatici relaziona al *Responsabile del trattamento* e altresì al C.I.S.I.A. per i casi che coinvolgano la sicurezza della Rete Unica della Giustizia (nel seguito RUG), sugli eventi e i comportamenti in difformità o in violazione del presente Piano o della normativa sulla sicurezza nella gestione del sistema informativo.
Per lo svolgimento di suddetti compiti, l'Amministratore Dei Servizi Informatici si avvale della collaborazione del personale del Servizio Assistenza Tecnica assegnato alle sedi giudiziarie con nota del Cisia Palermo 17028 del 24.06.2010, in particolare per;
- la stesura dell'inventario delle risorse hardware e software.

1.4 Incaricati del trattamento

Gli incaricati del trattamento, secondo l'art. 30 del "codice", sono i soggetti abilitati ad operare sui dati, sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni ricevute.
"La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima" (art. 30 co. 2 del "codice").
Tra gli incaricati è opportuno evidenziare una specifica e settoriale responsabilità in capo ai "funzionari" (o equiparati) titolari delle aree organizzative o dei singoli servizi giudiziari, che per comodità di seguito saranno indicati quali *Responsabili amministrativi.*

In particolare, con riferimento al trattamento dei dati, i *Responsabili amministrativi* devono farsi carico delle seguenti incombenze:
- proporre al *Responsabile del trattamento* il nominativo degli incaricati da accreditare, di coloro che devono essere disabilitati ed eventuali modifiche da apportare al profilo utente, in coerenza con le politiche di governo dell'ufficio;
- rilevare i fabbisogni informatici di area;
- curare il corretto utilizzo degli applicativi installati nella propria area, da parte degli incaricati/utenti, con particolare riferimento alla qualità dei dati inseriti nelle basi di dati;

- collaborare con l'Amministratore Dei Servizi Informatici, segnalando eventuali anomalie nella tenuta dei sistemi informativi;

- Va precisato che da ultimo c,o provvedimento del Dirigente amministrativo alcuni responsabili amministrativi sono stati nominati referenti del sistema con la precisa funzione di concedere le autorizzazioni all'accesso a coloro che ne facciano motivatamente richiesta e di inoltrarle al CISIA per le attività conseguenziali.

2. OBBLIGHI DI SICUREZZA

I dati personali oggetto di trattamento sono custoditi e controllati, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi,di accesso non autorizzato o di trattamento non consentito o non conforme alle finalita' della raccolta. i titolari del trattamento sono tenuti ad adottare le misure minime individuate di seguito, volte ad assicurare un livello minimo di protezione dei dati personali.-, come previsto dal D.Lvo 196/03 e descritto nel Discipèlinare di cui all'Allegato B di detto D.Lvo

A. Trattamenti con strumenti elettronici.

A.1 misure minime

Il trattamento con strumenti elettronici e' consentito solo se sono adottate, nei modi previsti da disposizioni legislative (disciplinare tecnico contenuto nell'allegato B D.Lvo 196/03),le seguenti misure minime:

a. **autenticazione informatica;**

b. **adozione di procedure di gestione delle credenziali di autenticazione;**

Il trattamento di dati personali con strumenti elettronici e'consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato,eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato,eventualmente associata a un codice identificativo o a una parola chiave.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

La parola chiave, quando e' prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e, successivamente, almeno

ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave e' modificata almeno ogni tre mesi.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Vanno adottate le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato, e precisamente;

- Sono personali
- Devono essere memorizzate
- Non devono essere comunicate a nessuno
- Non devono essere trascritte

In particolare:

- non rivelare le password a nessuno, inclusi amici e familiari
- non condividere le password con altri colleghi o assistenti
- non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono
- non scrivere le password su carta e non memorizzino le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura
- non scrivere la propria password su questionari o presunti moduli di sicurezza
- non parlare della propria password o rivelino indizi su essa
- non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password
- segnalare tutti i sospetti di compromissione o le richieste di informazioni sulle password (es. ultimo login non corrispondente ad orario di ufficio)
- non riutilizzino in nessun caso le password.

lo strumento elettronico durante una sessione di trattamento. non va lasciato incustodito e accessibile. gli Incaricati del trattamento hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.)

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso e' utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, e' verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Sistema di autorizzazione

Il **Responsabile di uno specifico trattamento di dati personali** ha il compito di individuare gli **Incaricati** del trattamento per ogni tipologia di banca di dati personali trattata.

In particolare il Responsabile di uno specifico trattamento di dati personali può decidere quali operazioni di trattamento siano consentite ad ogni Incaricato del trattamento tra le seguenti:

- Inserire nuove informazioni nella banca di dati personali;
- Accedere alle informazioni esistenti nella banca di dati personali;
- Modificare le informazioni esistenti nella banca di dati personali;
- Cancellare le informazioni esistenti nella banca di dati personali.

In conformità a quanto disposto dal punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. N. 196 del 30 giugno 2003) almeno una volta l'anno e comunque entro il 31 marzo, ogni Responsabile di uno specifico trattamento di dati personali deve aggiornare l'Elenco dei permessi di accesso che sono stati assegnati agli Incaricati del trattamento per ogni tipologia di banca di dati.

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

Gli utenti devono:
- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato;
- evitare di utilizzare giochi o software peer to peer (software che permettono la condivisione di files sulla rete i.e. Imesh, Gnutella, audiogalaxy, Napster software per le chat ICQ e simili);
- assicurarsi di non accendere al proprio computer con unità esterne di memoria rimovibili inserite. Infatti se queste fossero infette, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file. Per limitare i rischi connessi a questo comportamento in fase di installazione delle postazioni di lavoro è possibile impostare il BIOS in modo da avere come "primary boot device" il disco rigido di avvio e proteggere l'accesso al BIOS tramite password;
- proteggere i dischetti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- salvare o sottoporre a back-up i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:
- diffondere messaggi e-mail di provenienza dubbia o partecipare a "catene di S. Antonio" e simili. che possono generare traffico inutile (veri scopi di chi diffonde queste mail).
- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione antivirus;

- visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come richiamo per attirare visitatori su cui condurre attacchi informatici;
- modificare la configurazione del software antivirus.

Per ulteriori dettagli si rinvia al Manuale di sicurezza dell'utente.

A.2 Sicurezza dei Luoghi

a. Protezione delle aree e dei locali interessati

Le macchine server vanno collocate in un apposito locale (sala server).

La sala server deve essere dotata di:

1. Impianto antincendio adeguato a locali contenenti apparati informatici;
2. Impianto di condizionamento ambientale, opportunamente dimensionato;
3. Porte tagliafuoco e finestre blindate ove sia possibile accedere facilmente ai locali attraverso le finestre
4. Impianto elettrico a norma per il quale è stato segnalato dal responsabile del servizio prevenzione e protezione nel documento di valutazione dei rischi la richiesta di adeguamento che coinvolge l'intero palazzo;
5. Gruppo di continuità.

L'accesso alla sala server è consentito solo al responsabile del trattamento, o alle persone espressamente autorizzate dal procuratore Generale

In assenza del personale autorizzato, la sala server deve essere tenuta chiusa a chiave.

I supporti di backup vanno tenuti in armadi blindati, posti in locali distanti dalla sala server.

Tutte le chiavi vanno custodite dalla vigilanza o da personale delegato dal Capo dell'Ufficio.

Tutte le risorse necessarie per l'attuazione di quanto previsto in questa sezione sono individuate dal capo dell'ufficio, con l'intervento, ove necessario, del Procuratore Generale, nel suo ruolo di responsabile della sicurezza delle infrastrutture.

b. Gestione degli apparati di rete

Gli armadi che contengono gli apparati di rete vanno tenuti chiusi a chiave. Le chiavi vanno custodite secondo le procedure previste.

Le porte telematiche degli apparati di rete che non siano utilizzate saranno disabilitate tramite il software di gestione.

A.3 Altre misure di sicurezza

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati puo' essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e' almeno semestrale.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

A.4 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

1) I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

2) Vanno seguite e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

3) Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

4) Una misura indispensabile per tutti i server è di essere dotati di un gruppo di continuità (articolo 11 comma 3 DM 24/5/2001) per garantirne il funzionamento per un breve periodo anche in mancanza di alimentazione elettrica di rete. E' bene che il gruppo di continuità sia collegato al server in modo che se l'alimentazione di rete non viene ripristinata entro il tempo per cui il gruppo è dimensionato, allora venga effettuato automaticamente uno shutdown del sistema per evitare che possa danneggiarsi quando

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

A causa di guasti accidentali delle apparecchiature informatiche, dovuti a variabili esterne o dolose (sbalzi di tensione, incendi, attacchi deliberati, etc.), il rischio di perdita dei dati può essere notevole.
L'art. 10 del DM 24/5/2001 prescrive per ciascun ufficio idonee politiche e procedure per il salvataggio (backup) e per il recupero (recovery) dei dati, sia a livello di sistema sia a livello di database management system.
I dati da sottoporre a salvataggio o *back up* sono classificati in **dati di sistema** (necessari per il corretto funzionamento del sistema operativo, del *software* di base, del *database* management system, delle applicazioni installate, etc.) e **dati utente** (documenti, fogli elettronici, archivi di posta elettronica, ecc.).
Con riferimento all'art. 10 del DM 24/5/2001 commi 2, 3 e 4, si adottano le seguenti politiche di *back up*:
I dati presenti sui server ed i dati sensibili devono essere sottoposti a back-up completo con frequenza settimanale.
I back up dei nuovi dati o dei dati modificati devono essere effettuati con frequenza giornaliera, in maniera incrementale laddove possibile, altrimenti in maniera completa. E' possibile approntare anche un sistema giornaliero di back up incrociato fra i server, in aggiunta o in alternativa a quello su supporto rimovibile.

I file di log devono essere trattati come dati sensibili e quindi salvati periodicamente.
Per ogni supporto di back-up il costruttore specifica un numero massimo di operazioni di scrittura. Per evitare che un back-up risulti illeggibile, si raccomanda di non riutilizzare i supporti di back-up che sono stati riscritti un numero di volte pari al 95% di quanto raccomandato dal produttore.
Appena terminate le operazioni, i supporti di back-up devono essere riposti negli armadi di sicurezza, blindati ed ignifughi, collocati all'esterno delle sale server, nelle apposite sale di conservazione dei back-up, al fine di evitare accessi non autorizzati e trattamenti non consentiti . Tali armadi devono sempre essere mantenuti chiusi a chiave.
I supporti rimovibili contenenti dati sensibili o comunque essere resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
A richiesta dell'utente e compatibilmente con le esigenze di spazio sul server, per il back-up dei dati degli utenti sono messe a disposizione degli stessi, delle aree sui server dove gli utenti possono salvare i dati di cui desiderano sia fatto il back-up. La configurazione di ciascuna quota è tale da consentire l'accesso in lettura e scrittura solo ed esclusivamente all'utente proprietario e l'accesso in sola lettura all'Amministratore di sistema. E' cura di ciascun utente provvedere a copiare sulla propria quota i file che desidera sottoporre a *back up*.

B. Trattamenti senza l'ausilio di strumenti elettronici

Misure minime

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici e' consentito solo se sono adottate, nei modi previsti da disposizioni legislative (disciplinare tecnico contenuto nell'allegato B del D.Lvo 196/03), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) 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.

Modalità tecniche da adottare a cura del titolare, del responsabile,ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

- **UTILIZZARE LE CHIAVI!**

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, è opportuno chiudere a chiave l'ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

- **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**

Non bisogna lasciare che possano accedere alle stampe persone non autorizzate; se la stampante non si trova sulla propria scrivania bisogna recarsi quanto prima a ritirare le stampe. Le stampe vanno distrutte quando non servono più.

- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione,e sono restituiti al termine delle operazioni affidate.

- L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Adeguamento

Le disposizioni contenute nel disciplinare tecnico di cui all'allegato B del D.Lvo 196/03, relativo alle misure minime di sicurezza da adottare o, e' aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie ((e il Ministro per la semplificazione normativa)), in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Manuale per la Sicurezza

AD USO DEGLI INCARICATI

Introduzione

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione. Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:
Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;
Integrità: Le informazioni non devono alterabili da incidenti o abusi;
Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.
Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.
In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

LINEE GUIDA PER LA SICUREZZA

- **UTILIZZATE LE CHIAVI!**

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.
Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete Giustizia, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con il responsabile del trattamento dati del vostro ufficio.

NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile del trattamento dati.

APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;

COME PREVENIRE I VIRUS:

- **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
  Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO
Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

PROTEGGETE I VOSTRI DISCHETTI DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

COME *NON* PREVENIRE I VIRUS:

- **NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA**

  Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: i mail di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli *hoax* più diffusi).

NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

Linee guida per l'utilizzazione delle password

CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
6. NON usate il Vostro nome utente. È la password più semplice da indovinare
7. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

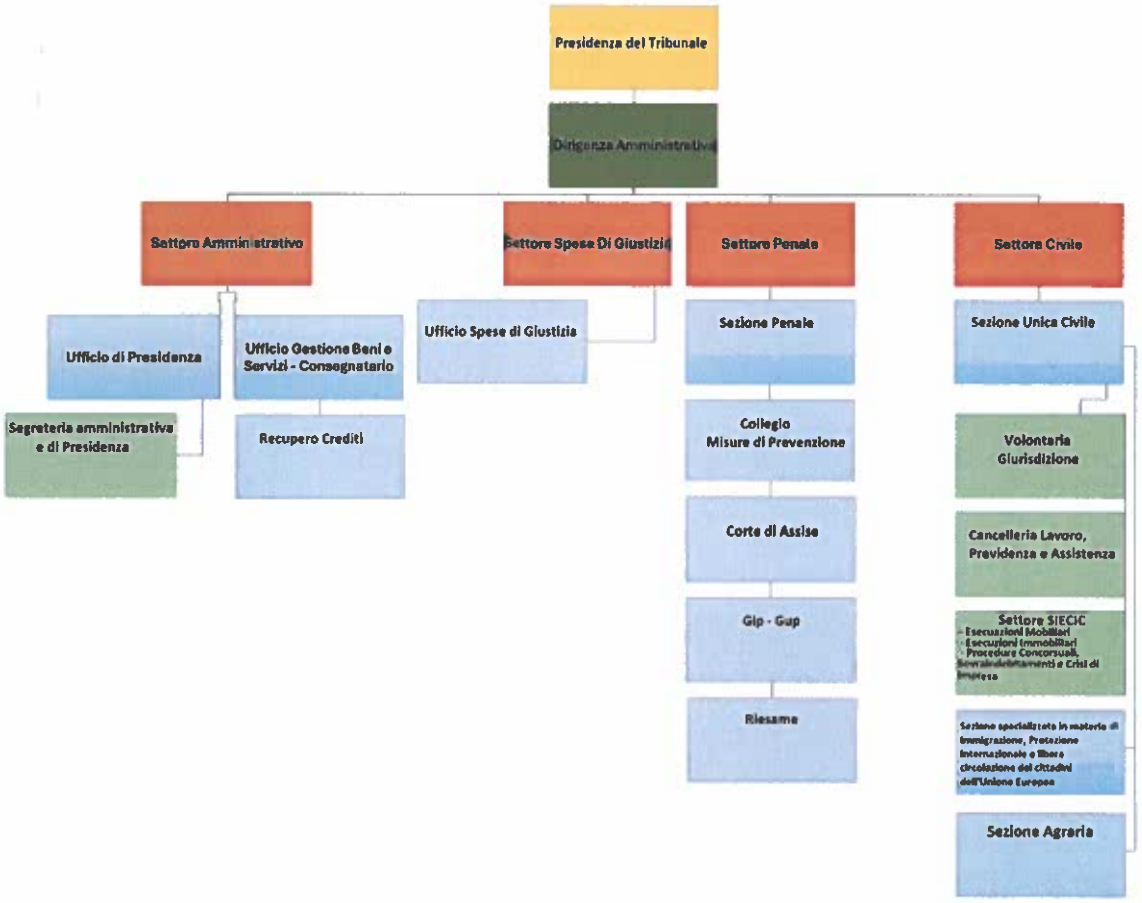
1. Cambiare la password a intervalli regolari. Chiedete al Vostro amministratore di sistema quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre mesi fino a due anni.
2. Usare password lunghe almeno sei caratteri con un misto di lettere, numeri e segni di interpunzione.
3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultate il vostro amministratore di sistema.

COME SCEGLIERE UNA PASSWORD

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degliincaricati puo' essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.



SETTORE AMMINISTRATIVO

PRESIDENTE DEL TRIBUNALE

DOTT. CESARE ZUCCHETTO

1- SEGRETERIA AMMINISTRATIVA E DI PRESIDENZA:

1	NATALE Daniela	direttore amministrativo- - responsabile
2	MANCUSO Katia	funzionario giudiziario
3	CANDURA Graziella	assistente giudiziario
4	CURATOLO Cinzia	assistente giudiziario
5	FARCHICA Filippa Erina	assistente giudiziario
6	RISORTO Maria	operatore giudiziario
7	SCARCIOTTA Leonardo Michele	operatore data entry
8	TALLUTO Alberto	conducente
9	FAVATA Calogera	ausiliario

- GESTIONE DEL PATRIMONIO: UFFICIO ECONOMATO E DEL CONSEGNATARIO:

1	LA VERDE VALENTINA	funzionario giudiziario-responsabile
2	PASSALACQUA Maria Teresa	tecnico di amministrazione
3	LA MAGNA Vincenzo Fabrizio	assistente giudiziario

- RECUPERO CREDITI

1	DI PIETRA Vincenzo	direttore amministrativo- - responsabile
2	MASTROSIMONE Tiziana	assistente giudiziario
3	FAVATA Calogera	ausiliario
4	INDORATO Maria	ausiliario

- SETTORE SPESE DI GIUSTIZIA

1	CHIPARO Giuseppe	funzionario giudiziario-responsabile
2	TRAMONTANA Sonia Tiziana	direttore amministrativo
3	TRAPANI Salvatore	operatore giudiziario
4	FAVATA Calogera	ausiliario
5	INDORATO Maria	ausiliario

SERVIZIO AUTOMEZZI

1	DI PIETRA Vincenzo	direttore amministrativo- - responsabile
2	ACQUISTI Guido	conducente
3	MARGAGLIONE Giuseppe	conducente
4	MICCICHE' Roberto	conducente
5	PETRONI Alberto	conducente
6	SABATINO Francesco	conducente
7	SORCE Giuseppe	conducente
8	TALLUTO Alberto	conducente

Servizi Penali

SEZIONE PENALE DIBATTIMENTALE

MONOCRATICO E COLLEGIALE

MAGISTRATI:

D'Arrigo Francesco Giovanni Maria (pres sez.)
Chianetta Giuseppina
Santacroce Lorena
Zappalà Giulia
N.N.
N.N.
Figliola Giuseppina (gop)
Milazzo Marco (gop)

PERSONALE:

1	PASTORELLO Luisa	direttore amministrativo- - responsabile
2	CANI Vincenza	funzionario giudiziario
3	CRISCUOLI Sergio	funzionario giudiziario
4	IACONA Giuseppe	funzionario giudiziario
5	FISICHELLA Desireè	funzionario giudiziario
6	LAPLACA Valeria Antonia	funzionario giudiziario
7	MAIRA Elvezia Annabella	cancelliere esperto
8	PERNA Germano	cancelliere esperto
9	BLANDINO Francesca	assistente giudiziario
10	FALETRA Edmondo	assistente giudiziario
11	PITRUZZELLA Vincenzo	assistente giudiziario
12	SCARPULLA Francesca	assistente giudiziario
13	SFERRAZZA Angela	assistente giudiziario

14	TRAINA Donatella	assistente giudiziario
15	FAVATA Calogera	ausiliario

COLLEGIO MISURE DI PREVENZIONE

1	SILITTI Cesare	funzionario giudiziario
2	LO PIPARO Tiziana	assistente giudiziario
3	VILLA Noemi	operatore data entry
4	FAVATA Calogera	ausiliario

CORTE DI ASSISE

1	PASTORELLO Luisa	direttore amministrativo- - responsabile
2	CANCEMI Elisa	funzionario giudiziario
3	PILATO Liboria	cancelliere esperto
4	FAVATA Calogera	ausiliario

GIP- GUP

1	LACAGNINA Sonia	direttore amministrativo- - responsabile
2	ALAIMO Ivan	funzionario giudiziario
3	GIANNAVOLA Lucio	funzionario giudiziario
4	NICOLETTI Lucia	funzionario giudiziario
5	SCADUTO Francesco	funzionario giudiziario
6	ALEO Roberta	tecnico di amministrazione
7	CASTELLANA Gianni Massimo	cancelliere esperto
8	TINAGLIA Concettina	cancelliere esperto
9	VULLO Letizia	cancelliere esperto
10	BURCHERI Rosanna	assistente giudiziario
11	CORTESE Giuseppa	assistente giudiziario
12	IANNELLI Fabiola	assistente giudiziario
13	MILANO Vincenzo	assistente giudiziario
14	IMPELLIZZERI Andrea	operatore giudiziario
15	LOMBARDO Federica	operatore data entry
16	RIGGIO Cettina	operatore data entry

17	TRUSCIA Rosa	operatore data entry
18	GANGI Alberto	operatore data entry - per 18 ore la settimana
19	RUSSOTTO Francesco	operatore data entry - per 18 ore la settimana
20	CORRAO Ignazio	conducente
21	MICCICHE' Roberto	conducente
22	INDORATO Maria	ausiliario

RIESAME

1	PILATO Angela	funzionario giudiziario-responsabile
2	CALABRESE Antonietta	cancelliere esperto
3	SAJEVA Manuela	cancelliere esperto - in aspettativa ai sensi dell'art 3, c.2, L. 51/2025
4	LO PICCOLO Francesco	assistente giudiziario
5	GIARDINA Elisabetta	assistente giudiziario
6	FAVATA Calogera	ausiliario

SETTORE CIVILE –

SEZIONE UNICA CIVILE

SEZIONE UNICA CIVILE - Collegio	1	Zucchetto Cesare (pres. Trib)
	2	N.N. (pres sez)
	3	Canto Gabriella (coord.sez)
	4	Lauricella Francesco
	5	Frasca Alessandra
	6	Guardo Giuliana
	7	Albergo Dario
		PERSONALE

1	GIANNONE Carola	direttore amministrativo- - responsabile
2	FERRARA Simona Micaela	funzionario giudiziario
3	MICCICHE' Fulvia	funzionario giudiziario
4	CAMMALLERI Vincenza Eliana	cancelliere esperto
5	DI LENA Graziella	cancelliere esperto
6	DI MARTINO Adriano	assistente giudiziario

7	FIORE Luigi	assistente giudiziario
8	MESSINA Fabiola	assistente giudiziario
9	PELONERO Laura	assistente giudiziario
10	AGNELLO Massimo	operatore giudiziario
11	CORDARO Giuseppe	operatore giudiziario
12	GANGI Alberto	operatore data entry - per 18 ore la settimana
13	LI PIRA Vanessa	operatore data entry
14	MESSINA Filomena	ausiliario
15	VITALI Giuseppe	ausiliario

VOLONTARIA GIURISDIZIONE

1	RABIOLO Nicolina	funzionario giudiziario-responsabile
2	RINALDI Stefania	funzionario giudiziario
3	PISA Eunice	funzionario giudiziario
4	CANNAROZZO Rosa	funzionario giudiziario
5	CORBO FEMMININO Valeria	cancelliere esperto
6	OCCHIPINTI Rossella	assistente giudiziario
7	RUSSOTTO Francesco	operatore data entry - per 18 ore la settimana
8	PETRONI Alberto	conducente
9	MESSINA Filomena	ausiliario
10	VITALI Giuseppe	ausiliario

Settore lavoro

1	CARUSO Rossana	direttore amministrativo- - responsabile
2	TESTAQUATRA Anna	funzionario giudiziario
3	VALENZA Antonella	funzionario giudiziario
4	CORSITTO Gianet	cancelliere esperto
5	GIUNTA Valeria	assistente giudiziario
6	FAVATA Calogera	ausiliario
7	INDORATO Maria	ausiliario

SEZIONE CIVILE - SETTORE SIECIC

1	MARCHESANO Vincenza	**funzionario giudiziario responsabile della cancelleria esecuzione mobiliare e referente coordinatore del settore SIECIC**
2	TORREGROSSA Giuseppe	assistente giudiziario
3	CALABRESE Maria Luisa	assistente giudiziario
4	AMICO Alida Emma	funzionario giudiziario responsabile della cancelleria esecuzione immobiliare
5	GALLINA Laura	funzionario giudiziario
6	GIACCHI Eleonora	tecnico di amministrazione
7	DI RAIMONDO Maria	funzionario giudiziario responsabile della cancelleria fallimentare
8	LIVECCHI Laura	cancelliere esperto
9	ROMITO Gero	operatore giudiziario
10	TRUPIA Tania	operatore data entry
11	VAIANELLA Antonella	operatore data entry
12	MESSINA Filomena	ausiliario
13	VITALI Giuseppe	ausiliario

SEZIONE CIVILE- Sezione specializzata in materia di immigrazione

1	GIANNONE Carola	direttore amministrativo- - responsabile
2	AMICO Filippa Simona	funzionario giudiziario
3	FALSONE Maria Elena	funzionario giudiziario
4	TUMMINELLI Giovanni	assistente giudiziario