Ministero della Giustizia

Dipartimento per la transizione digitale della giustizia, l'analisi statistica e le politiche di coesione

Direzione generale per i sistemi informativi automatizzati

Cisia di Napoli

Al Signor Procuratore presso il
Tribunale per i Minorenni
SALERNO

***Oggetto**: Informazioni in ordine alla gestione del sistema di protezione e sicurezza dell'infrastruttura informatica su cui alloggiano le istanze applicative ad uso del Tribunale, per ispezione in corso.*

I sistemi informatici di gestione dei registri civili (SICID) e di gestione dei registri penali (SIGMA) sono ospitati presso la Sala Server Interdistrettuale di Napoli.

Sotto il profilo della sicurezza informatica, è necessario considerare due aspetti:

1) *la sicurezza fisica dei locali e degli apparati tecnologici;*
2) *la sicurezza dei dati.*

Sicurezza fisica dei locali e degli apparati tecnologici.

Sala Server Interdistrettuale di Napoli

Al data center di Napoli si accede solo se identificati dalle aliquote di Polizia Penitenziaria e autorizzati dalla Procura generale partenopea che verifica eventuali precedenti in capo all'interessato.
Per giungere al locale macchine, devono superarsi due porte taglia-fuoco REI 120, lungo un percorso videosorvegliato. Gli accessi al Polo Informatico avvengono tramite badge e le porte sono controllate da due telecamere che convogliano le immagini alla sala regia del servizio di vigilanza ed è attivo H24 in conformità a quanto indicato dalle disposizioni della Procura Generale che è deputata alla sicurezza fisica degli uffici giudiziari del distretto.
All'interno della struttura vi sono due sale – una di produzione ed una di backup, presso cui sono alloggiati i rack ospitanti i server che gestiscono e contengono i dati. Ogni sala, per la continuità elettrica, è dotata di UPS di opportune dimensioni in modalità ridondante. Ogni UPS è alimentato da una linea elettrica indipendente e afferente al quadro elettrico dell'impianto con un proprio interruttore magneto-elettrico. Per completare l'affidabilità elettrica, vi è un gruppo di continuità elettrogeno - situato in una chiostrina distante circa 70 m - che entra in funzione quando vi è una prolungata mancanza di energia elettrica. Quindi, in caso di mancanza di energia elettrica, per un periodo di circa 20 minuti, gli UPS possono reggere il carico dei server continuando l'erogazione dei servizi mentre il gruppo entra in funzione a regime in uno-due minuti garantendo circa tre ore di autonomia. La manutenzione ordinaria e straordinaria del gruppo di continuità è in carico alla Direzione generale per le risorse materiali e tecnologiche.
Nei locali che ospitano i server sono presenti due telecamere di sorveglianza afferenti, come le altre, alla sala regia di cui sopra. Per il condizionamento dell'impianto si utilizza un impianto ridondante

e collegato all'impianto elettrico e al gruppo elettrogeno, in maniera da avere la continuità anche in mancanza di energia elettrica.

Sicurezza dei dati

Gli applicativi sono installati su macchine fisiche collocate in una infrastruttura in modalità di server virtuali.

Gli accessi, sia remoti che locali, all'infrastruttura presente nel data center è permessa esclusivamente al personale CISIA individuato con Ordine di Servizio dello scrivente o per effetto di contratti sottoscritti dalla superiore Direzione Generale SIA, per l'affidamento dei servizi di assistenza e gestione sistemistico-applicativa.

L'accesso ai sistemi informatici presenti nei data center avviene tramite profili caratterizzati da username e password (password con i previsti criteri di complessità e non ripetibilità), che sono registrati nel dominio nazionale ADN del Ministero della Giustizia; l'utenza ADN prevede il cambio della password obbligatoriamente ogni 180 giorni.

L'autenticazione dell'utente avviene direttamente su Active Directory e ad ogni utente è associato un profilo definito all'interno dell'applicativo stesso.

I profili di accesso sono autorizzati del titolare dell'Ufficio o suoi delegati.

Tali profili sono sempre modificali ed aggiornabili, su istanza formale dell'ufficio richiedente.

Una volta che la correlazione utente - profilo (ADN o applicativo) ha avuto esito positivo, l'utente, in base a specifiche policy di visibilità sui dati, dovute agli specifici profili, potrà usare l'applicativo solo per quanto autorizzato.

Per gli applicativi sono implementate politiche omogenee di backup, che rispettano quanto previsto dalle prescrizioni DGSIA, sia per i dati strutturati sia per i repository che contengono i documenti afferenti ai fascicoli. I backup giornalieri e i file di backup vengono dislocati su Server Virtuali e su Unità NAS presso la Sala Server Distrettuale per avere una ridondanza di sicurezza

Tutti i backup sono conservati in:

- *server di produzione,*
- *server differenti da quelli di produzione ospitati presso la sala server di backup di Napoli;*
- *sistema di archiviazione a lungo termine (Netbackup) e riversamento su supporti fuori linea (tape library).*

La storicizzazione riguarda anche la componente Repository che contiene i documenti che costituiscono il fascicolo. Tale componente è allocata sul sistema di produzione, sul sistema di archiviazione a lungo termine e sui nastri fuori linea.

L'accesso ai documenti avviene unicamente tramite gli applicativi e le politiche di profilazione degli utenti adottate dall'ufficio.

Ambito Penale

L'applicativo del settore penale (SIGMA) e i relativi archivi sono tutti ospitati presso la sala server nazionale di Napoli, installati su infrastruttura di server virtuali ospitati su macchine fisiche. L'accesso ai suddetti applicativi da parte del personale degli uffici giudiziari avviene mediante utenza ADN, previa autorizzazione del responsabile dell'ufficio che individua il perimetro di visibilità relativo sia alla visibilità sui dati che sulle funzioni/moduli dell'applicativo.

La gestione degli utenti e dei relativi profili è effettuata dal personale CISIA su richiesta del responsabile del trattamento; mediante appositi tools (consolle di amministrazione) disponibili per ogni applicativo, il personale CISIA e l'assistenza tecnica procede alle operazioni di configurazione dei vari moduli applicativi oltre che alla gestione delle utenze e delle tabelle di servizio.

Il personale CISIA accede agli applicativi per le attività di amministrazione (configurazione, profilazione utenti, ecc...); il personale dell'assistenza tecnica esterna accede mediante le credenziali ADN agli applicativi nonché mediante utenza DB, per le operazioni di manutenzione dei fascicoli, su richiesta dell'ufficio mediante apertura ticket) oltre che per le attività di aggiornamento a seguito di nuovi rilasci.

Ambito civile

L'infrastruttura tecnico-informatica dei sistemi di gestione informatizzata dei registri civili (SICID, SICID_UAC) e del sottosistema Processo Civile Telematico (PCT) è collocata presso la Sala Server Interdistrettuale del CISIA di Napoli. È presente, oltre all'infrastruttura di produzione, una infrastruttura di backup che contiene le copie dei dati e le informazioni necessarie ad eseguire il ripristino in caso di fault del sistema in produzione.

Gli utenti di cancelleria e i magistrati accedono ai dati solo attraverso l'applicativo ministeriale (SICID, SICID_UAC, Consolle del Magistrato, Consolle Civile del PM) con autenticazione ai sensi del DM 44/2011 art. 8.

Gli utenti abilitati esterni accedono ai dati in consultazione secondo quanto previsto dal DM 44/2011 artt.22 e succ.

Il personale del CISIA e dell'assistenza unificata accede ai dati tramite applicativo ministeriale e tramite la Consolle Unificata di Amministrazione che permette la gestione delle componenti di sistema del SICID, dei flussi del PCT e delle anagrafiche degli utenti del sistema SICID. La gestione degli utenti e della relativa profilazione è tecnicamente attuata dal personale CISIA su richiesta scritta e firmata del responsabile del trattamento dei dati del Tribunale.

Il personale CISIA e dell'assistenza accede inoltre alla componente Data Base con profilo che permette le operazioni di Read, Update e Delete (CRUD) sul DB (profilo necessario per poter procedere alle correzioni dei dati non effettuabili tramite applicativo). L'accesso alla componente DB avviene attraverso l'utilizzo di una c.d. 'macchina ponte' che filtra gli accessi in base a specifiche politiche firewall e rende disponibili sw autorizzati per l'esecuzione delle operazioni in parola.

Tutti gli accessi agli applicativi, sia ambito penale che civile, vengono tracciati e registrati in appositi file, c.d. "log applicativi", sottoposti a copia e archiviazione.

Per tutti gli applicativi vengono effettuati backup giornalieri e i file di backup vengono dislocati su Server Virtuali e su Unità NAS presso la Sala Server Distrettuale per avere una ridondanza di sicurezza.

Cordialità

Il Dirigente

Giovanni Malesci