Ministero della Giustizia

Dipartimento dell'Organizzazione Giudiziaria, del Personale e dei Servizi

Direzione Generale per i Sistemi Informativi Automatizzati

PIANO PER LA SICUREZZA INFORMATICA DELL'AMMINISTRAZIONE DELLA GIUSTIZIA

Informazioni sulla classificazione del documento

PIANO PER LA SICUREZZA INFORMATICA DELL'AMMINISTRAZIONE DELLA GIUSTIZIA				**Ver. 2.0**
Livello di classificazione		**Data di classificazione o di modifica alla classificazione**	**Responsabile della classificazione**	**Destinatari del documento**
Divulgabile (L1)				
Pubblico (L2)				
Circolazione limitata (L3)			Alessandra Cataldi	Personale del Ministero della Giustizia, relativi fornitori di sistemi e applicazioni informatiche
Circolazione ristretta (L4)				
Altamente riservato (L5)				

INDICE DEL DOCUMENTO

1 PREMESSA

Il presente documento, sostitutivo del piano strategico della sicurezza prot. 11606.ID del 13 dicembre 2018, è stato redatto all'esito di una lunga fase di:

1) consolidamento organizzativo indotto dal DPCM 84/2015 come modificato dal DPCM 99/2019 e dal DM del 23 aprile 2020. La revisione territoriale dei CISIA (Milano, Bologna, Roma, Napoli, Palermo) e la definizione di Uffici Dirigenziali (Ufficio per la governance economico-finanziaria, organizzativa e l'amministrazione aperta, Ufficio per la giurisdizione digitale territoriale civile e penale, Ufficio per la giurisdizione digitale nazionale civile e penale, Ufficio per i servizi digitali dell'amministrazione penitenziaria e della giustizia minorile e di comunità, Ufficio per l'amministrazione digitale, Ufficio per l'attuazione della trasformazione digitale, Ufficio per il coordinamento delle sale server e la sicurezza informatica, Ufficio per le reti, la connettività e l'interoperabilità, Ufficio per il procurement) hanno costituito la necessaria premessa di una politica di sicurezza indirizzata alla progettazione e al supporto degli uffici.
2) consolidamento delle infrastrutture sia centrali che periferiche (Sale server nazionali, interdistrettuali e distrettuali, locali tecnici, interventi sulle reti, potenziamento e cablaggio degli uffici), con riposizionamento strategico dei sistemi operativi ed applicativi.
3) consolidamento delle conoscenze con riferimento alla maturata estensione progettuale dei sistemi applicativi delle aree Penale, Civile e Amministrativa. Il DM 23 aprile 2020 (misure necessarie al coordinamento informativo ed operativo tra la Direzione generale per i sistemi informativi automatizzati del Dipartimento dell'Organizzazione giudiziaria, del personale e dei servizi e altre articolazioni del Ministero della giustizia, nonché individuazione degli uffici di livello dirigenziale non generale e definizione dei relativi compiti ai sensi dell'articolo 16, commi 1 e 2, del decreto del Presidente del Consiglio dei ministri 15 giugno 2015, n. 84 e dell'articolo 6, comma 2, del decreto del Presidente del Consiglio dei ministri 19 giugno 2019, n. 99) all'art. 4 comma 1 lettera c), attribuisce, tra gli altri compiti, alla Direzione Generale per i Sistemi Informativi Automatizzati il compito di predisporre e gestire il piano per la sicurezza informatica dell'Amministrazione della Giustizia relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso e alla conservazione dei documenti informatici, ai sensi del regolamento di cui al decreto del Presidente della Repubblica 28 luglio 1999, n. 318.

Se l'esigenza di una adeguata politica della sicurezza informatica si pone per ogni ente e amministrazione, ciò vale in particolar modo per l'Amministrazione della Giustizia. I dati che i suoi sistemi trattano, sia che riguardino direttamente la funzione giurisdizionale, sia che fungano da supporto amministrativo all'esercizio di tale funzione, sono comunque riconducibili ad un'attività fondamentale dello Stato, che deve essere preservata da intromissioni esterne ed esercitata sulla base di informazioni affidabili quanto alla loro integrità e provenienza, disponibili, nonché tutelate in relazione ai diversi gradi di riservatezza o sicurezza.Non tutti i dati hanno la medesima importanza e la medesima funzione. Inoltre, ciascun dato è trattato, unitamente ad altri, nell'ambito di specifici flussi di lavoro il cui risultato è in genere un altro dato. Ne consegue che la tutela della sicurezza dei dati deve prendere necessariamente in considerazione:

a) la struttura e le specifiche tecniche di conservazione fisica del dato;
b) la tipologia giuridica del dato;
c) il flusso di lavoro (ad esempio, la procedura amministrativa o il segmento di attività giudiziaria) all'interno del quale esso è processato.

L'analisi e la classificazione del dato deve tener conto, inoltre, dei diversi aspetti di politica di sicurezza da attuare, aventi come obiettivo la preservazione dell'integrità, della disponibilità e della confidenzialità del dato.

Per quanto attiene l'**integrità** del dato, devono essere attuati meccanismi di tutela che devono riguardare:

a) i dati classificati come segreti o riservati;

b) i dati la cui perdita totale o parziale incide sul funzionamento di un intero ufficio o settore di attività (ad esempio la perdita di un registro generale);

c) i dati la cui perdita o la cui ritardata produzione impone l'adozione di altre tecnologie per assicurare continuità temporale all'azione degli attori.

L'ultima classe di dati, oltre a postulare una valutazione giuridica nella classificazione degli atti, evidenzia come una corretta politica di sicurezza che tuteli l'esistenza del dato, la sua tempestiva produzione, la sua integrità sia rispetto a intrusioni esterne sia da errori di sistema, impatti positivamente anche sui tempi della giustizia, rendendo più spedito lo svolgimento della funzione giudiziaria e migliorando la qualità del servizio correlativo.

Relativamente alla **disponibilità** del dato, anche questa deve riguardarsi sia sotto il profilo fisico, sia sotto quello giuridico. In quest'ultimo ambito assumono rilievo gli atti soggetti a deposito in quanto l'inosservanza o l'ingiustificato ritardo di tale adempimento ha conseguenze processuali in grado di determinare l'arresto delle attività dell'unità organizzativa. Sono parimenti rilevanti i dati che la legge consente o impone di trasmettere a uno specifico organo pena l'inammissibilità, la decadenza, la nullità, l'inutilizzabilità, la perdita di efficacia (ad es., mancata trasmissione nel termine al tribunale del riesame, da parte del pubblico ministero, degli atti di cui all'art. 291, comma 1, c.p.p.) o altre sanzioni processuali incidenti su specifici atti o procedure, sanzioni da qualificarsi come rischi giuridici conseguenti alla mancata disponibilità del dato.

Infine, rispetto alla **confidenzialità** (**secretazione**) del dato, essa deve riferirsi ad una fase processuale rilevante ai sensi dell'art 329 c.p.p. e comunque alla sua conoscibilità per attori selezionati dalle dinamiche del processo, essendo necessario dare ingresso ad una fase di revisione delle politiche di gestione dei dati c.d. pubblici in ragione del mutato contesto tecnologico e della accresciuta sensibilità sociale.

Nel seguito saranno illustrate le misure di sicurezza che garantiscono, rispetto agli standard internazionali in merito, la conservazione di un livello di confidenzialità, integrità e disponibilità del dato compatibile con la natura dei dati giudiziari.

I destinatari del documento sono:

- il personale dell'Amministrazione della Giustizia, indipendentemente dai ruoli, inquadramenti, funzioni e responsabilità;
- i fornitori di sistemi e applicazioni informatiche, indipendentemente dalla natura specifica della fornitura. In tal senso, il documento deve essere esplicitamente sottoscritto per presa visione integrale da parte del fornitore.

Gli Uffici, cui sono demandate specifiche funzioni essenziali alla corretta implementazione delle politiche, sono tenuti a realizzare, nel rispetto della loro autonomia organizzativa, le misure previste dal presente documento mantenendo la maggiore standardizzazione e uniformità di implementazione possibile, per garantire omogeneità di presentazione delle procedure e collaborazione/interscambio di esperienze tra i vari Uffici.

2 NOTA METODOLOGICA

Le presenti politiche per la sicurezza dei sistemi informatici del Ministero della Giustizia sono state redatte seguendo un approccio metodologico *risk-based* alla sicurezza informatica, come suggerito dal Framework Nazionale per la Cybersecurity (FNCS).

In concreto, l'attività di stesura ha richiesto un'attività preliminare di modellazione dell'Amministrazione in classi di contesto, quali Ufficio Centrale, Ufficio Giudiziario e Sala Server, in cui le principali entità e unità organizzative del Ministero di Giustizia e dell'Autorità Giudiziaria sono state classificate. Per ogni classe sono stati individuati i livelli di sicurezza informatica definiti *critico*, *basso*, *medio* e *alto* per l'entità o l'unità organizzativa appartenente a tale classe. Un livello di sicurezza corrisponde a un elenco di misure di sicurezza informatica che un'entità o un'unità deve attuare per ridurre il rischio di esposizione a determinate minacce cyber.

Il livello *critico* è il livello minimo di sicurezza da raggiungere, in quanto una non totale attuazione delle misure previste per esso porterebbe l'entità o l'unità organizzativa inadempiente ad un'esposizione elevata al rischio di attacchi cyber. Di conseguenza, una volta coperto il livello minimo, più si implementano le misure previste per i livelli successi (basso, medio e alto), più il rischio di esposizione tende ad attenuarsi. I livelli di sicurezza di ogni classe di contesto individuata, e quindi le misure previste per tale classe, sono stati definiti tenendo in considerazione lo stato attuale delle minacce di rilievo per l'Amministrazione della Giustizia e le tecniche e le best practices presenti in letteratura in materia di sicurezza informatica e adottate in ambito nazionale e internazionale, atte a contrastare tali minacce. Quindi, è fondamentale che ogni entità o unità organizzativa dell'Amministrazione raggiunga, in un tempo ragionevole (obiettivo a breve termine), la copertura totale del livello critico previsto per la sua classe di appartenenza, di modo da ridurre in maniera considerevole l'esposizione alle attuali minacce cyber, e pianifichi (in un tempo medio o lungo) il raggiungimento della copertura dei rimanenti livelli di sicurezza previsti dalla stessa.

Il Documento delle politiche per la sicurezza dei sistemi informatici, quindi, è stato concepito con l'obiettivo di guidare l'Amministrazione della Giustizia nel far raggiungere una copertura totale del livello critico a tutte le entità e le unità organizzative in essa presenti in un tempo ragionevole, traducendo le misure di sicurezza previste per tale livello in politiche di sicurezza a priorità alta. Il Documento, inoltre, recepisce anche le misure previste per i livelli superiori (basso, medio e alto) sotto forma di politiche di sicurezza a priorità medio/bassa, la cui totale implementazione da parte di tutte le entità e le unità organizzative presenti nell'Amministrazione della Giustizia, porterebbe a una riduzione considerevole del rischio di esposizione alle attuali minacce cyber. Per cui, le priorità attribuite alle politiche di sicurezza sono intese come dei criteri che permettono di identificare preliminarmente quelle politiche che devono essere implementate per ridurre maggiormente i livelli di rischio a cui l'Amministrazione della Giustizia è sottoposta, bilanciandone l'impegno da profondere per la loro attuazione. In particolare, la determinazione dei livelli di priorità assegnati alle politiche è stata effettuata sulla base di due specifici criteri:

- *capacità di ridurre il rischio cyber*, agendo su uno o più dei fattori chiave per la determinazione, ovvero:
    - *esposizione alle minacce*, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
    - *probabilità di loro accadimento*, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
    - *impatto conseguente sulla continuità operativa o sugli asset*, intesa come l'entità del danno

conseguente al verificarsi di una minaccia;

- *semplicità di implementazione delle politiche di sicurezza*, anche considerando il livello di maturità tecnica e organizzativa tipicamente richiesto per realizzare la specifica azione.

Riportandosi all'introduzione, i tre livelli di priorità previsti per l'Amministrazione della Giustizia sono:

- **Alta**, che individua interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi;
- **Media**, che individua interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione;
- **Bassa**, che individua interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative).

3 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

In aggiunta ai termini definiti nelle norme e nella letteratura presenti nell'Allegato A, all'interno del documento si fa riferimento alle definizioni riportate nella tabella che segue.

Definizioni	
Mobile Endpoint Security	o Mobile Endpoint Protection è un approccio alla protezione delle reti a cui sono collegati dispositivi mobili quali laptop, tablet, smartphone e altri dispositivi wireless. Generalmente questo termine si traduce in politiche di sicurezza e strumenti come anti-virus, anti-malware, anti-spyware, anti-spam, firewall, HIPS, ecc. installati su dispositivi mobili presenti all'interno di una organizzazione, al fine di proteggere gli asset interni da minacce cyber che utilizzano i dispositivi mobili come vettore di attacco.
Workstation	Postazione di lavoro dei funzionari informatici, dei tecnici informatici o dei sistemisti
Postazione di Lavoro (PdL)	Postazione di lavoro di un utente (magistrato, cancelliere, amministrativo, ecc.) dell'Amministrazione della Giustizia
Cancellazione selettiva	Cancellazione dei dati contenuti in specifiche celle di memoria ROM, adottata in memorie EEPROM (Electrically Erasable PROM - memoria di tipo PROM cancellabile elettricamente)

Acronimi	
CAD	Codice dell'Amministrazione Digitale; il testo vigente è costituito dal DLgs 82/2005, e successive modifiche.
Dlgs	Decreto Legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
PLC	Politica di sicurezza
NAS	Network Attached Storage
ADN	Active Directory Nazionale
IPS	Intrusion Prevention System
HIPS	Host Intrusion Prevention System
IDS	Intrusion Detection System
NAC	Network Access Control

4 RUOLI E RESPONSABILITÀ DELLA SICUREZZA INFORMATICA

Lo svolgimento delle funzioni assegnate alla DGSIA coinvolge più soggetti, sia interni sia esterni (ovvero, di soggetti non gerarchicamente subordinati alla DGSIA, come ad esempio i magistrati e i dirigenti degli uffici giudiziari per l'accreditamento e l'autorizzazione all'accesso ai sistemi e per le operazioni che coinvolgono aspetti di sicurezza).

Ai diversi soggetti coinvolti sono attribuiti ruoli che si inseriscono nell'organigramma generale dell'organizzazione ai fini della sicurezza, integrando e arricchendo i ruoli e le procedure già previste per la gestione dei processi interni.

Per ogni figura prevista nel processo di gestione della sicurezza informatica sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così come è previsto che alcune attività possano essere svolte dal medesimo soggetto, è altresì previsto che alcune funzioni possano essere delegate ad altri soggetti, fermi restando i predetti vincoli di onorabilità e di requisiti di esperienza del delegato.

La gestione della sicurezza informatica all'interno della DGSIA coinvolge tutti i settori dell'organizzazione che interagiscono tra loro al fine di garantire il raggiungimento degli obiettivi di sicurezza prefissati. In particolare, le attività di gestione della sicurezza informatica impattano sulle seguenti funzioni organizzative:

- *Direttore Generale dei Sistemi Informativi Automatizzati presso il Ministero della Giustizia* (DG) nelle fasi di approvazione del piano della sicurezza e di suoi possibili aggiornamenti.
- *Responsabile della Sicurezza Informatica* presso la DGSIA (RS), se nominato dal DG (funzioni specificate nel resto del documento)
- *Responsabili della Sicurezza* presso le strutture territoriali di coordinamento interdistrettuale (RSD), se nominati dal DG (funzioni specificate nel resto del documento).
- *Incaricato o Referente della Sicurezza* (IS) presso una struttura dispiegata sul territorio (funzioni specificate nel resto del documento).
- *Fornitori di software di sistema e applicativo, fornitore di servizi di gestione tecnica e sistemistica dei sistemi e dell'infrastruttura, fornitore dei servizi di diffusione.*

La funzione di responsabile della sicurezza informatica (RS) è svolta dal DG, con facoltà di delegare tale funzione ad altro soggetto. Corrisponde alla figura apicale nella gerarchia delle responsabilità inerenti la sicurezza informatica dell'Amministrazione della Giustizia. Ha il compito di supervisionare, controllare e coordinare tutte le attività di programmazione, analisi, sviluppo, gestione e monitoraggio strettamente connesse alla sicurezza informatica, dei sistemi informativi e dell'infrastruttura di rete degli Uffici Centrali, degli Uffici Giudiziari e degli Uffici di diretta collaborazione del Ministro, del Dipartimento della giustizia minorile e di comunità e dell'amministrazione degli Archivi notarili, in coerenza con i requisiti di sicurezza predisposti dall'Amministrazione della Giustizia.

Alla figura del RS si affianca quella del responsabile della sicurezza informatica presso l'ufficio dirigenziale non generale di coordinamento interdistrettuale (RSD). Tale figura è nominata, con incarico ufficiale, dal RS (a cui risponde direttamente) ed è il responsabile delegato della sicurezza informatica per gli Uffici e le Sale Server dispiegati nel territorio di sua competenza. Ha il compito di supervisionare, controllare e coordinare tutte le attività di gestione, manutenzione e monitoraggio, strettamente legate alla sicurezza informatica, dei sistemi informativi e dell'infrastruttura di rete degli Uffici e delle Sale Server appartenenti all'area di sua competenza, in coerenza con i requisiti di sicurezza specifici per l'area.

È prevista inoltre la figura di incaricato/referente locale della sicurezza informatica. È la persona di

riferimento di un Ufficio Centrale, un Ufficio Giudiziario o una Sala Server, con la responsabilità di supervisionare, controllare e coordinare le attività di gestione e manutenzione tecnica e sistemistica, specifiche per la sicurezza informatica, dei sistemi informatici e dell'infrastruttura di rete, in conformità alle politiche e alle procedure di sicurezza previste per l'Ufficio o la Sala Server di sua competenza. Viene incaricata ufficialmente dal RDS con avallo del RS.

Nel seguito le funzioni attribuite al RS si intendono svolte dal DG qualora questi non abbia provveduto alla nomina di un RS.

Il DG, nel definire l'organigramma della struttura e assegnare mansioni e ruoli ai diversi soggetti coinvolti, specifica quali soggetti sono espressamente dedicati alla gestione della sicurezza informatica e ne definisce ruoli e responsabilità. Identifica i soggetti che, pur non appartenendo alla struttura della DGSIA, svolgono funzioni rilevanti ai fini della sicurezza informatica e definisce linee guida e buone pratiche di comportamento a essi destinate. Inoltre, nell'ambito del personale dell'organizzazione destinato alla gestione dei sistemi informatici, il DG deve definire quale di questo personale sia espressamente dedicato alla sicurezza informatica, specificando le relative responsabilità.

5 PERIMETRO DEL SISTEMA DI SICUREZZA INFORMATICA

Il RS è tenuto a identificare e a mettere in protezione i sistemi e gli apparati fisici che rientrano nel perimetro di sicurezza individuato dall'Amministrazione della Giustizia.

5.1 Definizione del perimetro del sistema di sicurezza informatica

5.1.1 Politica di gestione degli inventari delle risorse fisiche e logiche

Il RS deve mantenere una descrizione aggiornata dell'infrastruttura logica e fisica della rete e delle apparecchiature interconnesse, e deve predisporre delle procedure di monitoraggio automatico di detta infrastruttura al fine di verificarne la consistenza. Il RS, quindi, deve acquisire strumenti e sistemi software e definire opportune procedure operative affinché tutte le risorse (cioè, dispositivi, hardware, reti, dati e software) interne a un Ufficio Centrale, Ufficio Giudiziario e Sala Server siano censite e inventariate.

- **PLC-001 [alta]**: Il RS deve individuare e mettere in opera una suite di strumenti che permettono di censire e inventariare tutti i sistemi (PdL, workstation, server) e gli apparati fisici connessi alla rete interna di un Ufficio o di una Sala Server e a cui è associato un indirizzo IP. Tali strumenti devono permettere di tener traccia anche delle configurazioni attuali (al minimo la versione del Sistema Operativo o firmware installato, con eventuali aggiornamenti) e di quelle storiche. Il RS deve predisporre una procedura ufficiale di aggiornamento del sistema centralizzato che sovraintende all'inventario hardware e software automatizzato. Il RS deve inoltre predisporre le modalità di gestione e di controllo dell'inventario; tale inventario deve essere aggiornato ogni volta che nuovi sistemi e apparati approvati vengono collegati alla rete, registrandone almeno l'indirizzo IP del sistema o dell'apparato fisico. La suite di asset inventory utilizzata deve poter censire anche i dispositivi preposti alla sicurezza dell'informazione (es., Hardware Security Module - HSM, dispositivi di cifratura hardware e/o firmware, ecc.), e quelli specifici per il trasporto e la sicurezza dei dati in transito (es., switch, router, firewall, gateway, ecc.). Il RSD è tenuto a controllare e monitorare il corretto utilizzo di tali strumenti, secondo le procedure operative definite dal RS, per gli Uffici e le Sale Server di sua competenza, individuando un referente per categorie di sistemi e apparati fisici di sua diretta responsabilità. Inoltre, il RSD è tenuto a predisporre e gestire, sotto la supervisione del RS, un inventario di tutte le reti interne (comprese quelle eventualmente presenti per il monitoraggio e la gestione e distinte da quelle di produzione) degli Uffici e delle Sale Server di sua competenza, individuando, per ognuna di esse: il piano di indirizzamento; il piano di routing ed eventuali politiche di sicurezza per la limitazione del traffico; l'elenco delle VLAN e la corrispondenza col piano d'indirizzamento; l'elenco dei collegamenti punto-punto e l'elenco delle VPN. Il controllo e il monitoraggio della gestione di ogni singola rete sono delegati all'IS di competenza dell'Ufficio o della Sala Server in cui la rete è implementata.

- **PLC-002 [media]**: Il RS deve individuare e mettere in opera una suite di strumenti che permettono di gestire un elenco del software autorizzato (e la relativa versione) e necessario a ciascun tipo di sistema (PdL, workstation, server) e apparato fisico connesso alla rete degli Uffici e delle Sale Server. Il software deve essere catalogato in: SW commerciale e SW ad hoc (o "custom-made"/"made to order") per specifiche funzioni. Nella prima categoria devono rientrare i programmi applicativi o suite acquistabili o scaricabili gratuitamente e identificati come *Commercial Off-The-Shelf* (COTS), ovvero che non richiedono nessun ulteriore sviluppo/estensione software di adeguamento al contesto oltre alle configurazioni predisposte dal produttore. Nella seconda categoria, invece, rientrano tutti i SW sviluppati specificatamente per il contesto dell'Amministrazione della Giustizia; tale categoria racchiude ad esempio: SICP, TIAP, SIDNA, SIDDA SICID, PORTALE DEI CREDITORI, ecc., come

pure i sistemi SW sviluppati per il monitoraggio e l'analisi statistica. Il software deve essere successivamente classificato in: *stand alone*, ovvero che può essere eseguito in modalità autonoma (senza necessità di accedere alla rete) su una macchina isolata, oppure *network-based* le cui funzionalità richiedono l'utilizzo di una rete. In quest'ultimo caso, inoltre, il software deve essere catalogato in: *client-server*, cioè suddiviso in un componente *client*, che è in esecuzione su di una macchina client (es., una postazione di lavoro o una workstation), e in un componente *server* in esecuzione su una o più macchine server. *Web client-server*, ossia suddiviso in un componente web client che è in esecuzione su di una macchina client (es., una PdL o una workstation) e in un componente server, in configurazione di Web Application, in esecuzione su una o più macchine server. In quest'ultimo caso, deve essere inoltre distinta anche l'esposizione o meno a Internet e la classe di utenti che vi hanno accesso (anonimi/autenticati, interni di ruoli specifici, interni tutti, esterni). L'installazione di software non compreso nell'inventario deve essere consentita solo tramite esplicita autorizzazione del RS, e deve esserne tenuta traccia in un apposito inventario. Il RS deve predisporre inoltre una suite di strumenti informatici, per gli Uffici e le Sale Server, che consentono: (i) di eseguire giornalmente regolari scansioni sui sistemi (PdL, workstation, server), al fine di rilevare la presenza di software non autorizzato, e (ii) di gestire le configurazioni e i cambiamenti storici dei software autorizzati. Il RS deve inoltre individuare ufficialmente un referente per ogni software autorizzato dell'inventario, e deve definire, le modalità di gestione del suddetto inventario. Il RSD è in carico di controllare e monitorare il corretto impiego delle procedure impartite dal RS negli Uffici e nelle Sale Server di sua competenza.

- **PLC-003 [alta]**: Il RS deve mantenere un elenco di applicativi e strumenti di video-conferenza accessibili da specifiche PdL e workstation, eventualmente condivise tra più utenti, presenti negli Uffici e Sale Server, per la comunicazione e la collaborazione in tempo reale e in modalità interattiva fra diversi utenti dislocati remotamente in altri Uffici o Sale Server dell'Amministrazione. Il RS deve definire le modalità di gestione del suddetto inventario. Il RSD è in carico di controllare e monitorare il corretto impiego delle procedure impartite dal RS negli Uffici e nelle Sale Server di sua competenza.

- **PLC-004 [alta]**: Il RS è tenuto a censire tutte le applicazioni telematiche multicanale che favoriscono la comunicazione asincrona con altre PP.AA. e con cittadini e imprese. Il RS deve definire inoltre le modalità di gestione del suddetto inventario.

- **PLC-005 [alta]**:Il RS deve definire termini e modalità per la messa in sicurezza dei servizi, esposti tramite API, offerti dall'Amministrazione della Giustizia per le altre PP.AA., in accordo alle regole tecniche di sicurezza previste dal modello di interoperabilità di AgID. Il RS deve definire termini e modalità di gestione dell'elenco degli indirizzi di posta elettronica ordinaria (PEO) e di posta elettronica certificata (con riferimento al registro iPA) utilizzati per lo scambio di semplici email, email firmate, email cifrate e email certificate verso altre PP.AA..

- **PLC-006 [alta]**: Il RS è tenuto ad accertarsi che tutti i flussi di dati e le comunicazioni/notificazioni in ingresso e in uscita a un Ufficio Centrale, Ufficio Giudiziario o Sala Server siano censiti e documentati. Per ogni flusso e comunicazione/notificazione devono essere identificati e descritti i dati coinvolti e i ruoli dei mittenti e destinatari. Per i flussi e le comunicazioni/notificazioni ad un opportuno livello di criticità per l'Ufficio o la Sala Server, i dati coinvolti devono essere catalogati sulla base delle aree coinvolte (penale, civile e amministrativa) e dei livelli di confidenzialità, integrità e disponibilità.

- **PLC-007 [alta]**: Il RS è tenuto ad esercitare in proprio o in delega il controllo che tutti i sistemi informatici esterni (inclusi portali di altre PP.AA., provider di posta esterni, provider di data storing esterni, ecc.), con cui i sistemi interni ad un Ufficio Centrale, Ufficio Giudiziario o Sala Server (compresi Web browser, client di posta o specifici client di scambio informazioni/dati - es., Dropbox client, GDrive, ecc.) scambiano informazioni/dati/documenti, devono essere catalogati, comprese le loro configurazioni necessarie per l'interazione con essi (ad esempio, protocolli, interfacce applicative, indirizzi di rete, politiche di sicurezza, ecc.). Il RS deve incaricare ufficialmente un referente per ogni sistema esterno censito e deve definire un processo di gestione e controllo dell'inventario.

5.1.2 Politica di gestione delle priorità: risorse organizzative e logiche

Il RS deve provvedere affinché tutte le risorse (cioè, dispositivi, hardware, reti, dati e software) siano classificate e prioritizzate rispetto ai requisiti di confidenzialità, integrità, disponibilità e criticità richiesti da un Ufficio Centrale, Ufficio Giudiziario o Sala server di appartenenza.

- **PLC-008 [alta]**: Il RS deve stabilire delle modalità di classificazione dei dati rispetto alla confidenzialità (secretazione). La classificazione dovrebbe prevedere almeno i seguenti livelli: *bassa confidenzialità* (livello 1), *media confidenzialità* (livello 2) e *alta confidenzialità* (livello 3).

- **PLC-009 [alta]**: Il RS è tenuto ad individuare la protezione crittografica da applicare ai dati classificati ai livelli 2 e 3, prevedendo che la protezione crittografica del livello 3 sia più robusta rispetto a quella applicata al livello 2.

- **PLC-010 [media]**: Il RS deve stabilire delle modalità di classificazione dei dati rispetto alla disponibilità. La classificazione dovrebbe prevedere almeno i seguenti livelli: *bassa disponibilità* (livello 1), *media disponibilità* (livello 2) e *alta disponibilità* (livello 3). La classificazione deve tener conto del livello di disponibilità operativa utile agli utilizzatori del dato dell'Ufficio che ne è responsabile.

- **PLC-011 [alta]**: Il RSD deve verificare che tutte le risorse fisiche e logiche (hardware, dispositivi, reti, software) presenti negli Uffici e nelle Sale Server di sua competenza siano classificati in livelli di criticità che comprendono almeno i seguenti: *bassa criticità* (livello 1), *media criticità* (livello 2) e *alta criticità* (livello 3), secondo la procedura ufficiale di classificazione. La procedura di classificazione deve tener conto: (i) del livello di confidenzialità e (ii) del livello di disponibilità operativa assegnati al dato trattato dalla risorsa.

- **PLC-012 [alta]**: Il RS deve individuare ufficialmente un responsabile della classificazione delle risorse appartenenti agli Uffici e alle Sale Server. Il RS deve definire le modalità di priorizzazione delle risorse.

5.2 Protezione del perimetro del sistema di sicurezza informatica

Il RS definisce le modalità di controllo degli accessi relativamente ai soggetti incaricati della gestione dei sistemi e degli altri utenti.

5.2.1 Politica per il controllo degli accessi fisici

Il RS deve predisporre politiche e procedure per il controllo degli accessi fisici presso tutti gli Uffici Centrali, gli Uffici Giudiziari e le Sale Server dell'Amministrazione della Giustizia.

- **PLC-013 [alta]**: Il RS deve individuare, per ogni Sala Server, le tipologie di classi d'accesso fisico ai sistemi di elaborazione dati in esse presenti. Tali tipologie devono prevedere come minimo le seguenti classi: personale appartenente alla DGSIA (compreso quello del CISIA); personale di fornitori esterni; personale delegato dall'Amministrazione della Giustizia (ad esempio personale che esegue manutenzione/riparazione). Inoltre, il RS deve individuate le modalità di accompagnamento di eventuali visitatori e il rilascio di permessi temporanei a personale non appartenente alle categorie precedentemente elencate.
- **PLC-014 [alta]**: Il RS in collaborazione con i referenti responsabili degli Uffici competenti per materia, deve individuare le tipologie di classi d'accesso fisico ai sistemi di elaborazione dati in essi presenti, le modalità di accompagnamento di eventuali visitatori e il rilascio di permessi temporanei.
- **PLC-015 [alta]**: Il RSD deve individuare per ogni Sala Server di sua competenza, mediante opportuna documentazione tecnica, i perimetri dei locali in cui si trovano i sistemi informatici. Tali locali devono essere protetti da adeguati controlli di ingresso che garantiscono l'accesso al solo personale autorizzato e devono essere posizionati, all'interno dell'edificio, in modo che siano isolati dai punti di accesso per le consegne, le aree di carico/scarico e altri punti in cui persone non autorizzate possono entrare.
- **PLC-016 [bassa]**: Il RSD, in accordo con il RS, è tenuto a segnalare alla Direzione generale delle risorse materiali e delle tecnologie del Ministero di Giustizia, mediante l'organo della Conferenza Permanente, la necessità di un sistema software, qualora non presente, che consenta di tener traccia, tramite opportuni log, degli accessi del personale autorizzato presso i locali in cui si trovano i sistemi informatici delle Sale Server e/o dei locali tecnici di sua competenza. Tale sistema deve poter gestire anche lo storico degli accessi.

5.2.2 Politica per l'accreditamento dell'utenza e il controllo degli accessi logici

Il RS disciplina le modalità tecniche di accreditamento e profilazione delle utenze appartenenti all'Amministrazione della Giustizia, nonché quelle di modifica / revoca delle autorizzazioni concesse e di gestione delle registrazioni cronologiche (log).

Il RS individua le politiche di gestione e di amministrazione delle identità digitali e delle credenziali d'accesso per gli utenti e per i dispositivi dell'Amministrazione della Giustizia.

- **PLC-017 [alta]**: Il RS, in proprio o per delega, deve controllare che per ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server, le utenze di amministrazione di PdL, workstation, server, software e applicativi di sua diretta responsabilità, qualora queste non prevedano l'autenticazione a più fattori, devono utilizzare credenziali di almeno 14 caratteri. Inoltre, per tali credenziali, deve essere prevista una procedura di gestione del password aging e history, e devono essere impartite istruzioni sulla loro conservazione e gestione in modo da garantirne disponibilità e riservatezza.
- **PLC-018 [alta]**: Il RS, in proprio o delegando, deve controllare che per ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server, le utenze di amministrazione dei dispositivi hardware e di rete ivi presenti e di sua diretta responsabilità, qualora queste non prevedano l'autenticazione a più fattori, devono utilizzare credenziali di almeno 8 caratteri. Inoltre, per tali credenziali, deve essere prevista una procedura di gestione del password aging e history, e devono essere impartite istruzioni sulla loro conservazione e gestione, in modo da garantirne disponibilità e riservatezza.
- **PLC-019 [alta]**: Il RS, in proprio o delegando, deve mantenere l'inventario delle utenze di amministrazione di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata a operare e, nel caso non siano utilizzate da almeno

6 mesi, vengano disattivate, salvo quelle preventivamente autorizzate per scopi di gestione tecnica. Deve verificare inoltre che sia assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali devono corrispondere credenziali diverse, e che le utenze di amministrazione siano nominative e riconducibili a una sola persona.

- **PLC-020 [alta]**: Il RSD, coadiuvato dagli IS degli Uffici e delle Sale Server di sua competenza, deve verificare che le credenziali di autenticazione degli utenti che hanno accesso a dati personali consistono in un identificativo e una password, consegnata in maniera riservata, oppure in un dispositivo di autenticazione in possesso e a uso esclusivo dell'utente (es. smartcard), oppure in una caratteristica biometrica dell'utente. Inoltre la password di tali utenze deve essere composta da almeno 14 caratteri e deve essere cambiata almeno ogni 3 mesi.
- **PLC-021 [alta]**: Il RSD, in cooperazione con gli IS degli Uffici e delle Sale Server di sua competenza, deve vigilare che lo stesso codice identificativo usato per l'autenticazione (es. login name, username, etc.) non deve mai essere assegnato a due utenti diversi, nemmeno in tempi diversi. Inoltre, a ogni incaricato del trattamento deve essere associato un utente individuale; risulta pertanto vietata la condivisione di una stessa utenza tra più incaricati ed è vietato un qualsiasi suo utilizzo a chiunque non sia stato ufficialmente autorizzato a farlo.
- **PLC-022 [media]**: Il RS è tenuto a impartite istruzioni a tutto il personale sull'adozione delle necessarie cautele al fine di assicurare la segretezza delle credenziali di accesso e la diligente custodia dei dispositivi utilizzati per il trattamento, compresa la direttiva di non lasciare incustodito e accessibile lo strumento elettronico usato per il trattamento dei dati durante una sessione di trattamento.
- **PLC-023 [media]**: Il RS è tenuto a verificare che ogni sistema di gestione delle identità digitali degli utenti esterni all'Amministrazione della Giustizia (es., avvocati, cittadini, ecc.: non rientrano in questa categoria gli utenti esterni delle forze di Polizia Giudiziaria) sia integrato con il Sistema Pubblico per la gestione delle Identità Digitali (SPID), per l'accesso ai servizi telematici offerti dagli Uffici Giudiziari. Per i servizi applicativi offerti dall'Amministrazione della Giustizia in ambito SPC, invece, il sistema di gestione delle identità digitali deve utilizzare, per l'identificazione, le modalità previste dal sistema SPID e deve gestire gli accessi a (lista esaustiva):
    - servizi che non richiedono alcuna identificazione o autenticazione;
    - servizi che richiedono l'autenticazione in rete da parte di un'autorità di autenticazione;
    - servizi che richiedono, per le persone fisiche, l'identificazione in rete da parte di un'autorità di identificazione;
    - servizi che richiedono per gli utenti, oltre all'identificazione, l'attestazione di attributi e/o ruoli, che ne qualifichino ulteriormente le funzioni e/o i poteri.
- **PLC-024 [alta]**: Il RS deve verificare e controllare che, per ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server, la rispettiva gestione delle identità digitali, delle credenziali di accesso per gli utenti e dei profili di autorizzazione, deve avvenire per mezzo di sistemi informatici censiti dalla DGSIA. Il RS è tenuto inoltre a definire, per ogni sistema censito, le procedure tecniche di: creazione, aggiornamento e disattivazione di una utenza; configurazione dei sistemi per la generazione automatica della password per le nuove utenze, senza riferimenti riconducibili all'utente; configurazione del sistema per la modifica della password contestualmente alla prima autenticazione dell'utente, qualora la password sia stata generata automaticamente dal sistema, e configurazione per

la gestione di aging e history delle password possibilmente in maniera automatica. Il RS è tenuto a verificare, con cadenza almeno settimanale, che siano presenti aggiornamenti per i sistemi di gestione delle identità, degli accessi e delle autorizzazioni degli Uffici e delle Sale Server e, in accordo alla politica di gestione degli aggiornamenti dell'Amministrazione, provvedere alla loro installazione coadiuvato dai RSD e dagli IS dispiegati sul territorio.

- **PLC-025 [alta]**: Il RS deve verificare che le chiavi private di eventuali certificati digitali utilizzati all'interno di un Ufficio Centrale, Ufficio Giudiziario o Sala Server per operazioni di identificazione, autenticazione, autorizzazione, firma digitale e cifratura siano adeguatamente protette. In particolare, il RS deve controllare che vengano applicate tecniche di cifratura (con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit) o di hashing (con almeno l'applicazione dell'algoritmo SHA a 256 bit) per la protezione delle credenziali memorizzate nei sistemi di identificazione, autenticazione e autorizzazione censiti dalla DGSIA, e siano utilizzati dispositivi HSM (Hardware Security Module) o, alternativamente, smartcard e dispositivi USB, per la memorizzazione delle chiavi digitali utilizzate per tutte le operazioni di cifratura e firma digitale che avvengono nell'Amministrazione della Giustizia.
- **PLC-026 [media]**: Il RS deve predisporre per ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server una procedura che disciplina la gestione delle utenze (personale, applicazioni e dispositivi), dei ruoli, delle responsabilità e dei diritti d'accesso ai sistemi e ai servizi (definizione dei profili di autorizzazione). Tale procedura deve individuare anche le modalità di assegnazione dell'informazione segreta (es. password, certificati, ecc.) necessaria all'autenticazione delle utenze e le pratiche di conservazione della stessa. Inoltre, il RS è tenuto a rilevare alla Direzione di competenza il fabbisogno di un piano interno di formazione e aggiornamento su aspetti di sicurezza informatica attinenti la gestione del controllo degli accessi, in cui i percorsi formativi devono essere organizzati per funzione di lavoro (ruoli e responsabilità) e mirati su specifiche politiche e procedure organizzative e tecniche.

Il RS definisce le politiche di gestione e amministrazione dell'accesso alle risorse presenti nell'Amministrazione della Giustizia.

- **PLC-027 [alta]**: L'IS deve controllare che, a ciascuna utenza di amministrazione degli Uffici e delle Sale Server di sua competenza, vengano assegnati solo i privilegi necessari per svolgere le attività previste per essa, e queste utenze vengano utilizzate solo per effettuare le operazioni che richiedono i rispettivi privilegi. Inoltre, deve verificare che le utenze di amministrazione anonime come "root" su UNIX o "Administrator" su Windows siano utilizzate solo ed esclusivamente per situazioni di emergenza, e deve provvedere a gestire le relative credenziali in modo da assicurare l'imputabilità di chi ne fa uso.
- **PLC-028 [media]**: Il RS deve predisporre, per l'assegnazione dei diritti di accesso privilegiato in un Ufficio o Sala Server dell'Amministrazione, una procedura che seleziona il personale sulla base delle competenze richieste e della necessità operativa di modificare la configurazione dei sistemi.
- **PLC-029 [alta]**: Il RS definisce le procedure operative per la verifica che tutti gli accessi effettuati dalle utenze di amministrazione di un Ufficio Centrale, Ufficio Giudiziario o Sala Server siano registrati in appositi log.
- **PLC-030 [alta]**: Il RS predispone le procedure operative di definizione dei profili di autorizzazione, in modo da limitare l'accesso delle utenze alle sole informazioni (dati e documenti) necessarie per effettuare le operazioni di trattamento, in coerenza con il profilo di autorizzazione assegnato. La definizione dei profili deve tener conto della tipologia dei dati (dati personali, dati sensibili, dati

giudiziari, ecc.), della separazione delle funzioni istituzionali e delle aree di responsabilità individuate all'interno dell'Ufficio o della Sala Server, cosicché gli utenti possono accedere esclusivamente ai dati/documenti, alla rete, agli applicativi e ai servizi ai quali sono stati formalmente autorizzati ad accedere. Inoltre, il RS deve definire una procedura che disciplina la revisione periodica (almeno annuale) della sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati. In particolare, il RS dovrà individuare e incaricare differenti persone per la gestione dei sotto elencati servizi/sistemi per una PdL:

- Sistema di autenticazione (ADN);
- Sistema centralizzato di inventario hardware e software automatizzato;
- Sistema centralizzato anti-malware;
- Sistema centralizzato di installazione e aggiornamento software;
- Sistema centralizzato di supporto da remoto;
- Sistema centralizzato di logging.

- **PLC-031 [alta]**: Il RS deve disciplinare le operazioni di amministrazione (compresa anche la manutenzione) remota di server, workstation, NAS, dispositivi di rete e analoghe apparecchiature, in modo che esse vengano eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). Ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server deve applicare le modalità operative e gli strumenti con cui eseguire tali operazioni definiti e individuati da DGSIA.
- **PLC-032 [alta]**: Il RS deve impartire delle disposizioni tecniche che definiscono i criteri e i metodi di segregazione della rete interna a una Sala Server, nonché le modalità di segmentazione della stessa (es. VLAN/subnetting, DMZ, VPN, ecc.), tenendo conto del livello di sicurezza e di classificazione delle informazioni memorizzate su server e PdL connessi alla rete. Tali disposizioni devono tener conto che le informazioni con un determinato livello di segretezza devono essere confinate su segmenti separati, utilizzando firewall per filtrare il traffico tra i segmenti, e devono essere cifrate qualora vengono trasmesse attraverso segmenti non sufficientemente fidati. Inoltre, su tali reti non devono essere collegati dispositivi esterni al perimetro di sicurezza (ad esempio dispositivi personali).
- **PLC-033 [media]**: Il RS deve impartire delle disposizioni tecniche che definiscono i criteri e i metodi di segregazione della rete interna a un Ufficio, tenendo conto del livello di sicurezza e di classificazione delle informazioni memorizzate su PdL ed eventuali server connessi alla rete. Tali disposizioni devono tener conto che le informazioni con un determinato livello di segretezza devono essere confinate su segmenti separati, utilizzando firewall per filtrare il traffico tra i segmenti, e devono essere cifrate qualora vengono trasmesse attraverso segmenti non sufficientemente fidati. In particolare, le PdL devono essere attestate su reti dedicate e segregate da quelle sulle quali sono attestati server e dispositivi di rete, e su tali reti non devono essere collegati dispositivi esterni al perimetro di sicurezza (ad esempio dispositivi personali).
- **PLC-034** [**media**]: Il RS deve individuare procedure sicure per l'utilizzo di reti WiFi, indipendenti dalla Rete Giustizia, all'interno degli Uffici Giudiziari. Il RSD assicura che tali procedure siano adottate presso gli Uffici Giudiziari di propria competenza.
- **PLC-035 [alta]**: Il RS deve impartire delle istruzioni operative per la gestione degli ambienti di sviluppo, di test, di pre-produzione e di produzione, qualora presenti (ad esempio, devono essere esplicitate le tecniche di segregazione o segmentazione della rete che separano i tre ambienti; devono

essere definite le procedure operative di predisposizione di un ambiente e di passaggio da un ambiente all'altro, ecc.). Deve inoltre predisporre una procedura di incarico ufficiale di responsabilità per ciascuno dei tre ambienti.

Il RS individua le politiche che mirano a disciplinare il controllo degli accessi alle informazioni (dati/documenti) memorizzate o elaborate dai sistemi software presenti nell'Amministrazione della Giustizia.

- **PLC-036 [media]**: Il RS è tenuto a verificare che per ogni sistema software per il controllo degli accessi alle informazioni memorizzate ed elaborate da un Ufficio Centrale, Ufficio Giudiziario o Sala Server siano riportate, mediante opportuna documentazione ufficiale, le tecniche di gestione degli accessi che tale software implementa, ovvero:
  - *Discretionary* - DAC. Sistema basato su ACL. Questa tecnica viene utilizzata per limitare l'accesso alle informazioni basate sull'identità degli utenti e/o all'appartenenza a determinati gruppi. Le tecniche di accesso si basano tipicamente sulle autorizzazioni concesse a un utente in base alle credenziali presentate al momento dell'autenticazione (nome utente, password, token hardware/software, ecc.).
  - *Mandatory - MAC*. Sistema basato sui livelli di autorizzazione degli utenti generalmente rispecchianti la gerarchia organizzativa (es., livello 1, livello 2, livello 3, ...), una classificazione dei dati (es., segreto, segretissimo, riservato, riservatissimo, pubblico, ecc.) e una tabella di associazione, detta "security label", che lega i soggetti agli oggetti.
  - *Permission Based Access Control - PBAC*. Questo meccanismo è basato sul concetto di permesso. Un permesso può essere rappresentato semplicemente come una stringa, ad esempio "READ". L'accesso viene eseguito verificando che l'utente corrente abbia l'autorizzazione associata all'azione richiesta. L'associazione "*utente possiede un'autorizzazione*" può essere soddisfatta in maniera diretta creando una relazione tra l'utente e il permesso (chiamata *grant*) o in maniera indiretta. Nel modello indiretto, la concessione dell'autorizzazione è ad un'entità intermedia come ad esempio il gruppo di utenti. Un utente è considerato un membro di un gruppo di utenti se e solo se l'utente eredita le autorizzazioni del gruppo di utenti. Il modello indiretto semplifica la gestione delle autorizzazioni per un gran numero di utenti, poiché la modifica delle autorizzazioni assegnate al gruppo influenza tutti i membri ad esso appartenenti. In alcuni sistemi di controllo degli accessi basati su autorizzazioni e con un controllo accessi molto fine, ad esempio a livello di oggetto di dominio, le autorizzazioni possono essere raggruppate in classi. In questo modello si suppone che ogni oggetto di dominio possa essere associato a una classe che determina le autorizzazioni applicabili al rispettivo oggetto. In tale sistema, ad esempio, è possibile definire una classe "DOCUMENT" con le autorizzazioni "READ", "WRITE" e "DELETE"; una classe "SERVER" può essere definita con le autorizzazioni "START","STOP" e "REBOOT".
  - *Nondiscretionary* - anche detto *role-based access control - RBAC*. L'utente ha accesso ad un oggetto sulla base del ruolo attribuitogli: i ruoli sono definiti a partire dalle funzioni di lavoro, e i permessi vengono attribuiti rispettando l'autorità e le responsabilità derivanti dalla funzione di lavoro. Le operazioni su di un oggetto sono eseguite sulla base dei permessi. L'oggetto viene acceduto in base al ruolo dell'utente.
  - *Miscellaneous* - Una combinazione ad hoc delle precedenti tecniche.
- **PLC-037 [media]**: L'IS deve verificare che su tutte le workstation (postazione di lavoro dei funzionari informatici, dei tecnici informatici o dei sistemisti), i server e gli altri dispositivi (come ad esempio NAS - Network-Attached Storage), di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza, sia installato e/o attivato, nel rispetto della continuità operativa richiesta e

compatibilmente con l'architettura del sistema sottostante, un software, censito e approvato dalla DGSIA, che consenta la cifratura dei dati memorizzati localmente con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit.

- **PLC-038 [alta]**: Il RS deve verificare che vengano applicate tecniche di cifratura, con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit, per la protezione dei dati/documenti, classificati a un livello di segretezza elevato, ed elaborati e mantenuti dai sistemi applicativi (SICP, SIPPI, TIAP, Calliope, Script@, ecc.).
- **PLC-039 [alta]**: Il RS deve individuare tecniche e strumenti atti ad assicurare, soprattutto quando si utilizzano sistemi di file sharing di rete per la condivisione di documenti elettronici, che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementano le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.
- **PLC-040 [bassa]**: Il RS, coadiuvato dai RSD e dagli IS, deve individuare, in accordo alla normativa cogente, le necessità operative per l'abilitazione della scrittura di dati sui dispositivi esterni come HD esterni, CD/DVD, Pen Drive, ecc. per le workstation, i server e altri sistemi appartenenti a un Ufficio Centrale, Ufficio Giudiziario e Sala Server. Inoltre, il RS è tenuto ad impartire istruzioni tecniche per la gestione dell'inventario che tiene traccia dei sistemi interni ad un Ufficio o Sala Server abilitati a tale scrittura. Il RSD è tenuto a controllare la corretta applicazione delle suddette procedure negli Uffici e nelle Sale Server di sua competenza.
- **PLC-041 [alta]**: Il RSD deve controllare che le copie di sicurezza (backup) delle workstation, dei server e di altri dispositivi (come ad esempio NAS) appartenenti a un Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza avvengano mediante adeguata protezione fisica dei supporti utilizzati.
- **PLC-042 [media]**: Il RS deve impartire istruzioni tecniche per la cifratura delle copie di sicurezza (backup) di workstation, server e altri dispositivi (come ad esempio NAS) appartenenti a un Ufficio Centrale, Ufficio Giudiziario e Sala Server, qualora questi contengano dati/documenti classificati ad un livello di sicurezza elevato. Inoltre, nel caso i backup dovessero essere remotizzati su piattaforme cloud, indipendentemente dal livello di sicurezza delle informazioni contenute, queste devono essere cifrate con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit, prima della loro trasmissione.

5.2.3 Politica di gestione e manutenzione delle Postazioni di Lavoro (Digital Workspace)

Il RS è in carico di disciplinare le procedure di gestione delle postazioni di lavoro (PdL), avendo particolare riguardo alla: installazione e configurazione iniziale; installazione e aggiornamento del software di sistema; installazione e aggiornamento del software applicativo; limitazione alla connessione di supporti esterni o reti dati diverse da quelle appartenenti al perimetro di sicurezza e limitazioni alla modifica delle impostazioni da parte degli utenti. Il RS è tenuto a definire in collaborazione con gli organi competenti le classi di PdL presenti negli Uffici e nelle Sale Server dell'Amministrazione della Giustizia, individuando quelle di sua diretta responsabilità.

- **PLC-043 [alta]**: L'IS è tenuto a monitorare che su ogni PdL (compresi i PC portatili), di diretta responsabilità del RS, di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza, siano installati strumenti software (anti-malware, anti-virus, anti-spyware) censiti da DGSIA e atti a rilevare la presenza e bloccare l'esecuzione di malware, virus o spyware locali. Questi software devono

permettere anche il controllo dell'integrità dei file per verificare che il software e i file critici di una PdL (compresi gli eseguibili di sistema e le applicazioni sensibili, librerie e configurazioni) non siano stati alterati. L'IS deve monitorare inoltre che questi strumenti di rilevazione e verifica d'integrità vengano aggiornati frequentemente, possibilmente in maniera automatica e controllata da un software opportuno preposto per il controllo centralizzato delle PdL, e che le PdL siano configurate in modo che venga eseguita una scansione anti-malware, anti-virus e anti-spyware sui supporti removibili al momento della loro connessione con le stesse e sia disattivata l'esecuzione e l'anteprima automatica dei contenuti dinamici (es. macro) presenti nei file come pure l'apertura automatica di e-mail.

- **PLC-044 [alta]**: L'IS deve controllare che su tutte le PdL (compresi i PC portatili), di diretta responsabilità del RS, di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza siano installati e attivati firewall personali e/o sistemi IPS host-based censiti da DGSIA.
- **PLC-045 [alta]**: L'IS deve controllare che su tutte le PdL (compresi i PC portatili), di diretta responsabilità del RS, di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza sia installato e/o attivato un software, censito e approvato da DGSIA, che consente la cifratura, con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit, dei dati memorizzati su HD interni o su dispositivi removibili come HD esterni, CD/DVD, Pen Drive, ecc., e solo sui PC portatili o smartphone, sempre di diretta responsabilità del RS, di un software che consente la cancellazione remota di dati (remote wiping).
- **PLC-046 [alta]**: L'IS deve controllare che su tutte le PdL (compresi i PC portatili), di diretta responsabilità del RS, di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza deve essere installato un software di utilità per la sovrascrittura ripetuta dei dati. L'aggiornamento di tale software deve avvenire possibilmente in maniera automatica e controllata da un software opportuno preposto per il controllo centralizzato delle PdL.
- **PLC-047 [alta]**: Il RS deve verificare che l'accesso alle PdL (compresi i PC portatili), di sua diretta responsabilità, di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server deve avvenire mediante identificazione, autenticazione e autorizzazione sul sistema ADN (Active Directory Nazionale), utilizzando una password non inferiore agli 8 caratteri. Non sono ammesse identificazioni, autenticazioni e autorizzazioni mediante domini o workgroup locali. L'utilizzo di un sistema di Active Directory locale all'Ufficio o alla Sala Server come alternativa al ADN deve essere esplicitamente autorizzato dal RS. L'accesso alle PdL mediante utenze locali deve avvenire solo da personale ufficialmente autorizzato dal RS. Qualora non sia strettamente necessario per lo svolgimento dei compiti, l'accesso alle PdL deve avvenire per mezzo di utenze non dotate di privilegi di amministrazione. Nel caso in cui siano strettamente necessari privilegi di amministrazione, occorre comunque usare un utente privilegiato del dominio ADN.
- **PLC-048 [alta]**: L'IS deve controllare che le PdL, di diretta responsabilità del RS, di un Ufficio Centrale, Ufficio Giudiziario o Sala Server devono avere, in accordo alla normativa cogente e alle necessità operative, come configurazione standard la disabilitazione: (i) della scrittura di dati su dispositivi esterni come HD esterni, CD/DVD, Pen Drive, ecc. e (ii) delle tecnologie Bluetooth e NFC. L'abilitazione di tali funzionalità per una specifica PdL deve essere ufficialmente autorizzata e deve essere tracciata in un apposito inventario. L'uso dei dispositivi esterni e della tecnologia Bluetooth e NFC inoltre deve essere limitato a quelli necessari alle attività preposte e ufficialmente autorizzate.
- **PLC-049 [alta]**: L'IS deve controllare che le copie di sicurezza (backup) delle PdL appartenenti a un Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza avvengano mediante adeguata

protezione fisica dei supporti utilizzati.

- **PLC-050 [bassa]**: L'IS deve controllare che venga applicata una cifratura, con almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit, dei dati contenuti nelle copie di sicurezza (backup) delle PdL appartenenti a un Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza, qualora queste contengano dati/documenti classificati ad un livello di sicurezza elevato. Inoltre, nel caso i backup dovessero essere remotizzati su piattaforme cloud, l'IS deve controllare che sia applicata la cifratura delle copie prima della loro trasmissione, indipendentemente dal livello di sicurezza attribuito alle informazioni contenute in esse.

- **PLC-051 [alta]**: Il RS deve impartire istruzioni tecniche di configurazioni sicure standard per la protezione dei Sistemi Operativi e delle applicazioni in esecuzione sulle PdL di sua diretta responsabilità. Il RSD deve verificare che tali istruzioni siano correttamente attuate in ogni Ufficio e Sala Server di sua competenza. Tali configurazioni devono subire adeguate operazioni di "hardening", ad esempio: l'attivazione di un *reference monitor* configurato con ADN o con un sistema alternativo ufficialmente autorizzato dal RS per il controllo degli accessi ai file locali della PdL, utilizzo di una password per l'accesso al bios delle PdL, utilizzo di funzioni di time-out su inattività della PdL, eliminazione degli account non necessari, disattivazione o eliminazione dei servizi non necessari, configurazioni di stack e head non eseguibili, applicazione di patch, chiusura delle porte di rete non utilizzate, ecc. Prima del collegamento alla rete di una PdL, inoltre, le credenziali dell'amministratore predefinito devono essere sostituite con valori coerenti a quelli delle utenze di amministrazione in uso nel contesto di riferimento. Le immagini d'installazione delle PdL devono essere memorizzate offline in un repository gestito centralmente e devono essere conservate in modo da garantirne l'integrità e la disponibilità solo agli utenti autorizzati. Devono essere previste configurazioni differenti per differenti tipologie di PdL presenti nell'Ufficio Centrale, Ufficio Giudiziario e Sala Server. Il RS è tenuto ad impartire istruzioni agli utenti sull'utilizzo delle PdL, in particolare di non lasciare incustodita la PdL, di renderla non accessibile (blocco o log out) in sua assenza, impostando un timeout dopo il quale la PdL non utilizzata viene bloccata automaticamente. Il RSD è tenuto a verificare la corretta attuazione di tali istruzioni negli Uffici e nelle Sale Server presenti nell'area di sua competenza.

- **PLC-052 [alta]**: Il RS deve predisporre una procedura di gestione delle configurazioni e degli aggiornamenti delle PdL. Il RSD è tenuto a verificare, sotto la sua responsabilità, la corretta implementazione della suddetta procedura negli Uffici e nelle Sale Server di sua competenza.

- **PLC-053 [alta]**: Il RS è tenuto ad acquisire strumenti informatici e impartire relative istruzioni tecniche affinché le patch e gli aggiornamenti del sistema operativo e delle applicazioni per le PdL, di sua diretta responsabilità, siano gestiti e installati automaticamente da un software opportunamente preposto per il controllo centralizzato delle PdL. Deve inoltre predisporre delle istruzioni tecniche per gli aggiornamenti specifici delle PdL (compresi PC portatili) separate dalla rete. Deve individuare una suite di strumenti informatici e definire delle procedure operative per la gestione e il controllo della manutenzione remota delle PdL. Il RSD è tenuto a verificare, sotto la sua responsabilità, la corretta implementazione delle suddette procedure negli Uffici e nelle Sale Server di sua competenza.

- **PLC-054 [bassa]**: Il RS deve individuare una suite di strumenti informatici e definire delle procedure operative per la gestione del ripristino dell'accesso ai dati presenti nelle PdL di sua diretta responsabilità, in caso di danneggiamento o perdita involontaria degli stessi, in tempi non superiori a sette giorni. Deve inoltre definire delle procedure di gestione e di conservazione dei log, e di

manutenzione e riparazione delle PdL. Il RSD è tenuto a verificare, sotto la sua responsabilità, la corretta implementazione delle suddette procedure negli Uffici e nelle Sale Server di sua competenza.

- **PLC-055 [alta]**: Il RS è tenuto a definire le procedure ufficiali di aggiornamento dei software censiti da DGSIA e preposti per: (i) la rilevazione automatica della presenza di malware, virus o spyware sulle PdL e del blocco della relativa esecuzione; (ii) l'installazione degli aggiornamenti e delle patch sulle PdL; (iii) la manutenzione remota delle PdL.
- **PLC-056** [**media**]: Il RS individua opportuni strumenti software di mobile endpoint security, ai fini della completa protezione degli strumenti mobile (laptop, smartphone, ecc.) di produttività.

5.2.4 Politica di gestione e manutenzione dei sistemi e apparati fisici

Il RS è tenuto a disciplinare la gestione delle installazioni, delle configurazioni e della manutenzione dei sistemi (workstation, server, NAS, switch, router, ecc.) interni a un Ufficio Centrale, Ufficio Giudiziario e Sala Server.

- **PLC-057 [alta]**: Il RS deve individuare una serie di configurazioni sicure standard per la protezione dei Sistemi Operativi in esecuzione su workstation, server, NAS o altro dispositivo presente in un Ufficio Centrale, Ufficio Giudiziario e Sala Server. Tali configurazioni sicure standard devono permettere di proteggere i sistemi operativi e le applicazioni in esecuzione sui sistemi di cui sopra, mediante adeguate operazioni di "hardening", come: l'attivazione di un *reference monitor* configurato con ADN o con un sistema alternativo per il controllo degli accessi ai file locali del sistema (workstation, server e NAS), utilizzo di funzioni di time-out su inattività del sistema; utilizzo di firewall host-based configurati in modo da scartare per default tutto il traffico di rete eccetto quello associato a porte e servizi esplicitamente autorizzati; eliminazione degli account non necessari; disattivazione o eliminazione dei servizi non necessari; configurazioni di stack e head non eseguibili; applicazione di patch e fix di sicurezza; chiusura delle porte di rete non utilizzate; disabilitazione dell'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili. Le immagini d'installazione di tali sistemi devono essere memorizzate offline in un repository gestito centralmente, e devono essere conservate in modo da garantirne l'integrità e la disponibilità solo agli utenti autorizzati. Devono essere previste configurazioni differenti per le differenti tipologie di workstation, server e altri dispositivi. Inoltre, il RS deve impartire le istruzioni operative e tecniche (i) sulla sostituzione delle credenziali di amministrazione predefinite con valori coerenti a quelli del contesto di riferimento, prima di un collegamento alla rete di una workstation, un server, un NAS, o un qualsiasi altro dispositivo, e (ii) sulla custodia e sull'utilizzo di dispositivi esterni che deve essere limitato a quelli necessari alle attività istituzionali. Infine, il RS deve stabilire i casi di utilizzo dei supporti esterni rimovibili, le tipologie di operazioni possibili e le tecniche di cifratura da adottare (almeno l'applicazione dell'algoritmo AES con chiavi a 256 bit). Il RSD deve monitorare la corretta applicazione delle suddette procedure e istruzioni operative negli Uffici e nelle Sale Server di sua diretta responsabilità.

- **PLC-058 [media]**: Il RS deve definire una procedura ufficiale che disciplini la gestione delle configurazioni dei sistemi (workstation, server o altro dispositivo) e degli aggiornamenti specifici per i sistemi separati dalla rete, in particolare per quelli air-gapped, adottando misure adeguate al loro livello di criticità. Deve definire inoltre una procedura che disciplina la gestione e il controllo della manutenzione remota per i suddetti sistemi (workstation, server, NAS, switch, router, ecc.), e deve adottare idonee misure per garantire il ripristino dell'accesso ai dati presenti in essi, in caso di

danneggiamento o perdita involontaria degli stessi, in tempi non superiori a sette giorni. Deve definire infine una procedura che individui le modalità per la gestione e il controllo dei log per tali sistemi e per la manutenzione e la riparazione degli stessi. Il RSD è responsabile di verificare la corretta implementazione delle suddette procedure negli Uffici e nelle Sale Server di sua competenza.

Il RS deve predisporre un'adeguata politica di backup dei dati adottata dall'Amministrazione della Giustizia.

- **PLC-059 [alta]**: L'IS deve monitorare che venga effettuata, almeno settimanalmente, una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino di server o NAS e che i supporti, contenenti almeno una delle copie, non siano permanentemente accessibili dal sistema stesso onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza. Inoltre, l'IS deve controllare che i backup dei dati personali siano eseguiti almeno settimanalmente, e verificare l'utilizzabilità delle suddette copie di sicurezza mediante ripristino di prova. Per i dati ritenuti altamente critici per l'operatività di un Ufficio o di una Sala Server, l'IS deve monitorare che ne sia effettuato, almeno quotidianamente, il completo backup.
- **PLC-060 [media]**: L'IS, se richiesto, è tenuto a controllare che l'esecuzione di un'attività di cancellazione selettiva dei dati, mediante opportuni strumenti informatici censiti dalla DGSIA, garantisca la non ripristinabilità dei dati cancellati.
- **PLC-061 [alta]**: L'IS è tenuto a verificare che venga applicata la cifratura AES con chiavi a 256 bit per la protezione delle copie di backup di dati classificati ad un livello di segretezza elevato per l'Ufficio o la Sala Server di appartenenza dei suddetti back-up.

5.2.5 Politica di gestione dei software applicativi

Il RS è tenuto a disciplinare le attività di gestione e manutenzione dei software applicativi di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server, definendo politiche e linee guida.

- **PLC-062 [media]**: Il RS deve controllare che per ogni software applicativo installato in un Ufficio Centrale, Ufficio Giudiziario o Sala Server venga gestita e mantenuta la relativa documentazione tecnica di dettaglio, mediante opportuni software documentali censiti dalla DGSIA. La gestione documentale deve tener conto delle due distinte categorie di software: commerciale e ad hoc. Per i software commerciali deve essere mantenuta e gestita la documentazione tecnica ufficiale fornita dal produttore e quella inerente l'installazione e la configurazione specifica di contesto, mentre per il software ad hoc dovrà essere mantenuta e gestita la documentazione tecnica di proprietà dell'Amministrazione della Giustizia, rilasciata, tramite procedura ufficiale, dal corrispondente fornitore, compresa di manuale d'installazione e configurazione. Per entrambe le tipologie di software, la documentazione tecnica dovrà contenere il blueprint dell'applicativo, descrivendo dettagliatamente i diversi livelli software che lo costituiscono, ovvero:
    - *Il livello base*. In questa categoria rientra: il sistema operativo compreso di versione, aggiornamenti e configurazioni specifiche, nonché i servizi di sistema attivi richiesti come ad esempio TCP, UDP, SNMP, IPsec, SMTP, ecc.; l'ambiente di runtime (es., Java Virtual Machine, Common Language Runtime, Node.js, interprete Python, interprete PHP, ecc.), con eventuali Container manager (es. Docker) e le rispettive versioni e configurazioni. Per le configurazioni, deve essere esplicitamente indicato se è stata adottata una configurazione consigliata dal produttore (individuando quella scelta) o, invece, una personalizzata (in tal caso, si dovrà riportare il dettaglio della configurazione).

- *Il livello middleware*. In questa categoria rientrano: Server Web e/o Web container (es., Apache web server, Tomcat, ecc.), Application server (es., Red Hat JBoss, Oracle WebLogic Server, IBM Web Sphere, ecc.), Enterprise Service BUS (es., Oracle ESB, IBM Integration Bus, ecc.), Process management system (es., TIMBO BPM, Oracle SOA Suite, IBM Process Server, ecc.), Content management system (es., MS SharePoint, Oracle WebCenter Content, IBM ECM, Liferay, WordPress, Joomla!, Drupal, ecc.), Document management system (es., Alfresco, LogicalDOC, M-Files, KRYSTAL, FileNet, ecc.) compresi di versione, aggiornamenti e configurazioni. Anche in questo caso si dovrà riportare il dettaglio delle configurazioni messe in opera, in particolare, l'adozione di configurazioni consigliate (individuando quella scelta) o, invece, personalizzate (in tal caso, si dovrà riportare il dettaglio della configurazione applicata).
- *Il livello di persistenza o di storage*. In questa categoria rientrano: database management system (es., Oracle Database, MongoDB, MSSQL Server, MySQL, IBM DB2, ecc.), file system locali o distribuiti compresi di versione, aggiornamenti (es., eventuali patch applicate) e configurazioni (es., RAC). Anche in questo caso si dovrà riportare, nel manuale d'installazione, il dettaglio delle configurazioni implementate, in particolare, l'adozione di configurazioni consigliate (individuando quella scelta) o, invece, di quelle personalizzate (in tal caso, si dovrà riportare il dettaglio della configurazione adottata).

Per i componenti e/o moduli dei software applicativi prodotti ad hoc e sviluppati da terze parti, la documentazione tecnica di dettaglio rilasciata dal fornitore dovrà riportare, esplicitamente: i file eseguibili o interpretabili (es., zip, war, ear, phy, sh, bat, exe, yaml, ecc.), compresi degli script di configurazione; la tecnologia di base utilizzata nella realizzazione di tali componenti e/o moduli (es. .NET, Java, Javascript, plug-in MS Office, ecc.) con la versione delle librerie di base utilizzate per lo sviluppo di tali componenti e/o moduli; la configurazione di questi ultimi nel corrispondente ambiente di runtime, e degli eventuali servizi remoti che tali componenti/moduli necessitano per il loro corretto funzionamento (es., servizio HTTP o HTTPS, FTP o SFTP, Remote File, Remote DBMS, ecc.) con le rispettive configurazioni. Inoltre, sempre per i servizi remoti, la documentazione dovrà riportare in maniera dettagliata la configurazione delle credenziali per l'accesso remoto utilizzato dal componente e/o modulo, eventuali altri parametri richiesti dal servizio (es., tipo di protocollo utilizzato, porta, indirizzo di rete o di dominio, ecc.) e come tali parametri sono memorizzati in maniera persistente o temporanea sulla macchina locale in cui tali componenti sono installati. Infine, dovranno essere individuate le cartelle e i file locali o presenti su un server remoto di scrittura dei log del componente e/o modulo, riportando i parametri di configurazione per l'accesso remoto a tali cartelle come pure la modalità di memorizzazione (temporanea o persistente) di tale informazione.

Inoltre per i software catalogati come network-based, la documentazione tecnica di dettaglio dovrà riportare informazioni sui protocolli di comunicazione sicuri adottati, quali: PGP, S/MIME, HTTPS, SFTP, SSL/TLS, IPsec, ecc., con la corrispondente versione utilizzata e le particolari configurazioni di sicurezza applicate per lo specifico caso, come ad esempio: la tipologia di certificato digitale e la Certificate Authority che l'ha rilasciato (interna o esterna all'Amministrazione della Giustizia); metodo di compressione e suite di codici (che definisce l'algoritmo per lo scambio delle chiavi, l'algoritmo di cifratura e di MAC - Message Authentication Code); l'identificativo ID di sessione e altre informazioni. Inoltre, in riferimento a

ogni protocollo, si devono riportare le librerie di base richieste e installate nella macchina ospitante tale software e supportanti tale protocollo (es., OpenSSL, OpenSSH, ecc.).

Per ogni software applicativo di un Ufficio Centrale, Ufficio Giudiziario e Sala Server devono essere documentate le tecniche di sicurezza implementate a supporto della confidenzialità, dell'integrità e della disponibilità (CIA) delle informazioni trattate (es., dati, documenti elettronici, file multimediali, ecc.). In particolare, devono essere esplicitate in documentazione le tecniche di cifratura a supporto della confidenzialità e dell'integrità dei dati gestiti dal sistema, come pure le tecniche di memorizzazione temporanea (es., caching, cartelle temporanee, ecc.) e persistente degli stessi (es. configurazione della sicurezza dei DBMS, dei File distribuiti, ecc.) e delle eventuali informazioni a supporto (es., funzioni hash, checksum, chiavi di cifratura, ecc.). Per la gestione dell'informazione segreta (es. password, chiavi, ecc.) utilizzata dal sistema per la cifratura e l'hashing dell'informazione, si deve tener traccia delle tecniche utilizzate per la confidenzialità, l'integrità e la disponibilità della stessa implementate nel software (cifratura di tali informazioni, l'algoritmo implementato e chiavi utilizzate), e la tecnologia di conservazione utilizzata (es. DBMS, HSM, ecc.).

Per ogni software, la documentazione tecnica dovrà contenere i dettagli sulle tecniche di autenticazione utilizzate, con riferimento ai livelli di sicurezza definiti dallo standard internazionale ISO in materia di autenticazione [ISO/IEC 29115:2013, standard recepito da UNI CEI ISO/IEC 29115:2015], ovvero:

- *Livello di sicurezza 1 (LoA1)*: il sistema non implementa meccanismi di autenticazione. Questo è il caso in cui la sola informazione di identificazione dell'entità consente l'accesso al sistema, ovvero non si implementa nessuna tecnica di controprova. Esempi sono: un indirizzo di posta elettronica o altro identificativo; l'indirizzo MAC della scheda di rete, ecc.
- *Livello di sicurezza 2 (LoA2)*: il sistema implementa tecniche di autenticazione a un fattore, come ad esempio una password associata a un identificativo. Questa tecnica può essere evoluta mediante l'utilizzo di metodi crittografici (es., Digest access authentication) per la protezione delle credenziali in transito sulla rete.
- *Livello di sicurezza 3 (LoA3)*: il sistema implementa tecniche di autenticazione a due fattori, non basati necessariamente su certificati digitali (es., password e One Time Password associati alla digitazione di una UserId). In generale, tali sistemi applicano un primo metodo che si riferisce a "una cosa che sai" (per esempio una password o un PIN), e un secondo scelto tra "una cosa che hai", come un telefono cellulare, una casella postale (elettronica e non) o un oggetto fisico come un token, e "una cosa che sei", come l'impronta digitale, il timbro vocale, la retina o l'iride, o altre caratteristiche di riconoscimento attraverso caratteristiche uniche del corpo umano (biometria).
- *Livello di sicurezza 4 (LoA4)*: il sistema implementa tecniche di autenticazione a due fattori, basati su certificati digitali e utilizza dei dispositivi di custodia delle chiavi private che soddisfano i requisiti dell'Allegato II del regolamento eIDAS.

Inoltre, la documentazione dovrà indicare:

- i protocolli di autenticazione implementati, ovvero:
    a) *Autenticazione tramite password* (Password Authentication Protocol (PAP), Challange Handshake Authentication Protocol (CHAP), One-time password e Encrypted Key Exchange).
    b) *Autenticazione tramite challenge* (protocolli definiti dagli standard ISO/IEC 9798-2 e ISO/IEC 9798-4).

c) *Autenticazione con algoritmi asimmetrici*, (protocollo standard ISO/IEC 9798-3).
d) *Zero-knowledge proof* (protocollo Fiat-Shamir).
e) *Miscellaneous*, una combinazione dei precedenti protocolli.
f) *Altri*, specificare il tipo di protocollo.

- gli eventuali metodi crittografici utilizzati a supporto dei protocolli di autenticazione, come ad esempio le funzioni hash (es., MD5, SHA-1, SHA-2, ecc.) e la relativa lunghezza (es., 128, 224, 256, 384, 512 bit), la tipologia di chiavi utilizzate (es., simmetriche, asimmetriche, effimere, ecc.) e i meccanismi di conservazione delle stesse.

- **PLC-063 [media]**: Il RS deve predisporre una procedura di rilascio da parte dei fornitori della documentazione tecnica e del codice sorgente dei software applicativi di proprietà dell'Amministrazione della Giustizia.

- **PLC-064 [alta]**: Il RS deve verificare che le patch dei prodotti e dei software applicativi degli Uffici e delle Sale Server siano valutate nell'ambiente di test prima di essere installate nei sistemi in esercizio. Inoltre, il RSD è tenuto a verificare che l'attività di verifica della presenza di patch per i software degli Uffici e delle Sale Server di sua competenza sia eseguita regolarmente, con una cadenza non superiore ai 6 mesi.

- **PLC-065 [alta]**: Il RS è tenuto a individuare gli strumenti e definire le procedure per il rilascio di aggiornamenti e patch dei software applicativi. Tali procedure devono inglobare istruzioni operative per la preparazione degli ambienti di test e pre-produzione, e quelle di passaggio in produzione dei nuovi aggiornamenti o delle nuove patch. Il RSD è in carico della supervisione della corretta applicazione delle procedure nei contesti di sua competenza.

5.2.6 Politica di gestione delle comunicazioni

Il RS definisce i criteri e le modalità di riservatezza delle comunicazioni al fine di preservare la confidenzialità delle informazioni trasmesse.

- **PLC-066 [alta]**: Il RS deve garantire che: (i) gli scambi dei dati/informazioni/documenti verso e da altre PP.AA. devono avvenire mediante porta di dominio (fino a sua totale dismissione) o, alternativamente, con protocollo TLS nella versione più recente disponibile oppure, ove questo non fosse possibile, almeno nella versione 1.2, e adottando una mutua autenticazione attraverso l'uso di certificati X509 v3, e (ii) lo scambio di messaggi di posta elettronica crittografati e firmati digitalmente verso e da altre PP.AA. devono avvenire sulla base dello standard S/MIME e PGP.

- **PLC-067 [alta]**: Il RS deve garantire e controllare che la trasmissione di dati/documenti classificati a un livello di segretezza elevato deve aver luogo solo su reti protette, e mediante l'adozione di opportuni protocolli per la cifratura del canale trasmissivo come IPSec e TLS (almeno alla versione v1.2 con AES-256 bits e SHA-2) e attraverso comunicazioni cifrate punto-punto effettuate a livello delle applicazioni, come: HTTPS, con almeno TLSv1.2 e AES-256/SHA-2 o RSA-2048/SHA-2; SFTP e SCP entrambi con protocollo SSH-2 con almeno AES-256/SHA-2 o RSA-2048/ SHA-2.

- **PLC-068 [alta]**: Il RS deve assicurare e controllare che la trasmissione, mediante posta elettronica ordinaria, di dati/documenti classificati a un livello di segretezza elevato può avvenire solo se il dato/documento è cifrato con opportune tecniche di cifratura a chiave asimmetrica come: PGP/GPG, con almeno RSA-2048/SHA-2, e S/MIME v3.2, entrambi con certificati X.509 v3. Qualora venga utilizzato PGP/GPG come canale alternativo a S/MIME, il dato/documento, prima di esser allegato al

messaggio criptato di posta elettronica, deve essere cifrato con almeno RSA-2048/SHA-2.

- **PLC-069 [alta]**: Il RS deve assicurare che il sistema di protocollo informatico dell'Ufficio Centrale, dell'Ufficio Giudiziario e della Sala Server, qualora previsto, deve:
    - assicurare l'univoca identificazione e autenticazione degli utenti e la protezione delle informazioni relative a ciascun utente nei confronti degli altri oltre che garantire l'accesso alle risorse esclusivamente agli utenti abilitati;
    - prevedere la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione. Deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
    - consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni devono essere protette da modifiche non autorizzate;
    - rispettare le misure di sicurezza previste dalla normativa cogente in materia di protezione dei dati personali.

  Il RS deve verificare che il registro giornaliero di protocollo venga trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
- **PLC-070 [media]**: Il RS deve assicurare che il sistema di gestione della PEC degli Uffici e delle Sale Server deve essere conforme alle regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata, in accordo all'art. 48 comma 3 del CAD e s.m.i.
- **PLC-071 [media]**: Il RS deve controllare che il sistema utilizzato dal fornitore accreditato dell'Amministrazione della Giustizia per la generazione di riferimenti temporali relativi ai messaggi (busta E-gov), scambiati nell'ambito dell'interazione tra servizi applicativi SPC e mediante porta di dominio se non ancora dismessa, deve garantire stabilmente uno scarto non superiore al decimo di minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.
- **PLC-072 [media]**: Il RS deve provvedere alla definizione dei requisiti degli applicativi in termini di protocolli di comunicazione ammessi al fine di garantire la riservatezza della trasmissione. Inoltre deve acquisire sistemi e strumenti informatici che permettano di monitorare e controllare i canali di comunicazione, quali e-mail, sistemi di instant messaging (IM), VoIP, internet, accessi wireless, al fine di preservare la confidenzialità e l'integrità delle informazioni in transito, e allo stesso tempo a impedire l'abuso che si potrebbe fare di tali strumenti di comunicazione.

5.2.7 Politica di gestione, dismissione e smaltimento degli apparati e dei supporti

Il RS definisce le politiche di gestione per la dismissione/distruzione degli apparati e dei supporti rimovibili come HD esterni, CD/DVD, Pen Drive, DAT, LTO, ecc.

- **PLC-073 [alta]**: Il RS deve definire una procedura che disciplini il trasferimento fisico, la rimozione e la distruzione dei dispositivi fisici (compresi i supporti rimovibili come HD esterni, CD/DVD, Pen Drive, DAT, LTO, ecc.) atti al trattamento e/o alla memorizzazione di dati interni a un Ufficio Centrale, Ufficio Giudiziario e Sala Server. La procedura di dismissione e smaltimento deve tener conto del livello di riservatezza del dato contenuto all'interno del dispositivo. Inoltre, per i supporti rimovibili contenenti dati sensibili o giudiziari, se riutilizzati da altri incaricati non autorizzati al trattamento degli stessi dati, le informazioni precedentemente in essi contenute devono essere rese non

intelligibili e non ricostruibili in alcun modo. Devono essere inoltre individuate le modalità di distruzione dei dati che tengono conto dei diversi livelli di riservatezza.

5.2.8 Politica di gestione e manutenzione dei servizi tecnici e impianti

- **PLC-074 [media]** Il RSD deve mantenere e gestire un'adeguata documentazione, il cui schema è redatto dal RS, relativa alle apparecchiature tecniche presenti all'interno degli Uffici e delle Sale Server di sua competenza e necessarie per garantire il corretto funzionamento degli apparati (Rif.[**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**]), con particolare riferimento a una:
  - descrizione dettagliata delle caratteristiche degli UPS per garantire continuità del servizio;
  - descrizione degli impianti di condizionamento, delle finalità specifiche relative sia al funzionamento ordinario sia alle eventualità di disastro e della relativa manutenzione;
  - descrizione degli impianti antincendio e della relativa manutenzione;
  - descrizione dell'infrastruttura fisica di rete (cavi, cablaggi, ecc.) e della relativa manutenzione.

6 MONITORAGGIO E CONTROLLO

Il RS è tenuto a disciplinare, mediante apposite politiche e procedure, il monitoraggio dei sistemi e degli apparati fisici presenti nell'Amministrazione della Giustizia, e l'acquisizione e la conservazione di opportuni log in modo che quest'ultimi siano utilizzabili per fini giudiziari.

6.1 Politiche e procedure di monitoraggio e controllo

Il RS definisce le misure di monitoraggio e di controllo del funzionamento dei sistemi dell'Amministrazione della Giustizia ai fini della sicurezza informatica di concerto con i RSD.

- **PLC-075 [bassa]**: Il RS deve individuare degli strumenti informatici da mettere in opera sul perimetro di una rete interna ad Ufficio o una Sala Server che consentano (i) il monitoraggio di tentativi di esfiltrazione, ad esempio tramite l'utilizzo di canali cifrati come TLS e SSL, delle informazioni classificate a un livello di segretezza elevato, (ii) di bloccare il trasferimento di tali informazioni fuori dal perimetro della rete e segnalare l'incidente al personale di sicurezza e (iii) di rilevare e filtrare il codice malevolo prima che raggiunga gli host (PdL, workstation, server o altro dispositivo) presenti in una rete. Il RS deve provvedere inoltre all'individuazione di strumenti SIEM (Security Information and Event Management) per monitorare, aggregare e correlare gli eventi provenienti da molteplici sorgenti, quali host (macchine fisiche e virtuali), apparati di rete (router, switch, ecc.), firewall, IDS e IPS presenti in una rete. Infine, il RS deve definire una procedura per il test regolare degli strumenti e dei sistemi di monitoraggio (quali firewall, IDS, IPS, SIEM, ecc.), per esempio prevedendo delle attività di test di penetrazione eseguiti almeno una volta l'anno, attraverso prove di intrusione dall'esterno con l'ausilio di personale esperto (c.d. tiger team), con la finalità di verificare la tenuta dei sistemi. Il RSD deve monitorare il corretto utilizzo degli strumenti e i sistemi di cui sopra all'interno delle reti degli Uffici e delle Sale Server di sua diretta responsabilità.
- **PLC-076 [bassa]**: Il RS deve individuare strumenti informatici quali IDS/IPS, filtri antispam e meccanismi di whitelisting/blacklisting su file e domini web, che consentano il filtraggio del contenuto dei messaggi di posta e del traffico web interni alla rete RUG. Deve individuare, altresì, i gestori della blacklist di url e le modalità di gestione della stessa.
- **PLC-077 [alta]**: Il RS deve individuare una suite di strumenti software anti-malware, anti-virus e anti-spyware per PdL, workstation, server o altri dispositivi interni ad un Ufficio o una Sala server, atti a rilevare la presenza e bloccare l'esecuzione di malware, virus o spyware, nonché strumenti in grado di verificare, in qualsiasi forma, l'aggiornamento dei software di cui sopra. Il RS deve altresì definire delle configurazioni opportune degli strumenti di monitoraggio di cui sopra per una scansione anti-malware, anti-virus e anti-spyware sui supporti removibili al momento della loro connessione con workstation, server o dispositivi vari, in modo che sia disattivata l'esecuzione e l'anteprima automatica dei contenuti dinamici (es. macro) presenti nei file come pure l'apertura automatica di e-mail. Gli strumenti anti-malware, anti-virus e anti-spyware individuati devono prevedere inoltre tecniche di controllo dell'integrità dei file per verificare che il software e i file critici di una workstation, server o altro dispositivo (compresi gli eseguibili di sistema e le applicazioni sensibili, librerie e configurazioni) non vengano alterati.
- **PLC-078 [alta]**: Il RSD deve verificare che tutti i punti di accesso fisico ai locali dove risiedono i sistemi informatici presenti nelle Sale Server di sua competenza, siano monitorati costantemente da personale di sicurezza e/o attraverso apparati di sorveglianza e allarmi che registrano i log di accesso in tali locali su opportuni file.

- **PLC-079 [alta]**: Il RS deve individuare dei strumenti di monitoraggio quali firewall personali o sistemi IPS host-based, e definire le rispettive configurazioni per workstation, server o altro dispositivo presente in una rete. Tali strumenti di monitoraggio devono essere gestiti centralmente e non deve essere consentito agli utenti non amministratori di alterarne la configurazione.
- **PLC-080 [media]**: Il RS è tenuto a definire opportune configurazioni per i sistemi di sua diretta responsabilità e presenti in una rete di un Ufficio o di una Sala Server, e di dotarsi di strumenti informatici che consentono di controllare che su tali sistemi siano in esecuzione soltanto le applicazioni e i processi indispensabili e censiti per quel dispositivo, con la verifica che soltanto le porte previste siano effettivamente in uso.
- **PLC-081 [alta]**: Il RS deve individuare idonei strumenti software e definire opportune istruzioni operative volti a controllare e monitorare a livello centrale o territoriale, tramite IS, l'uso e i tentativi di utilizzo di dispositivi esterni non autorizzati all'interno di un Ufficio o di una Sala Server, rilevando e impedendo l'accesso alla rete ai dispositivi (anche quelli wireless) non autorizzati.
- **PLC-082 [alta]**: Il RS, di concerto con i RSD, deve predisporre per gli Uffici e le Sale Server una suite di strumenti software che consentano di automatizzare il processo di scansione delle vulnerabilità su tutti i sistemi presenti in una rete interna, e che fornisca a ciascun amministratore di sistema un report con indicazioni delle vulnerabilità più critiche rilevate. Inoltre, devono essere individuate le modifiche significative delle configurazioni dei sistemi, o la frequenza periodica, in cui è necessario eseguire il processo di vulnerability scanning (almeno settimanalmente). Gli strumenti adottati devono essere aggiornati con frequenza regolare e devono essere eseguiti in modalità privilegiata da un account dedicato che non viene utilizzato per nessun'altra attività di amministrazione. Almeno una volta l'anno, devono essere eseguiti test di penetrazione con l'ausilio di personale esperto (c.d. tiger team), con la finalità di verificare la tenuta dei sistemi.
- **PLC-083 [bassa]**: Il RSD, con l'avallo del RS, deve nominare ufficialmente un referente per i processi di monitoraggio della rete e dei sistemi, di analisi degli eventi di sicurezza e di reporting per ogni Ufficio e Sala Server di sua competenza. Inoltre, il RSD, con approvazione del RS, deve predisporre un processo di miglioramento continuo dell'attività di monitoring che si avvale anche delle conoscenze acquisite dall'analisi degli incidenti passati.
- **PLC-084 [alta]**: Il RS deve predisporre un piano per notificare tutte le violazioni relative alla privacy dei dati personali all'autorità di controllo senza ingiustificato ritardo, ai sensi dell'articolo 30 della Direttiva UE 2016/680, ed un piano per comunicare, senza ingiustificato ritardo, le violazioni relative alla privacy dei dati personali direttamente all'interessato qualora la violazione rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'articolo 31 della Direttiva UE 2016/680.
- **PLC-085 [media]**: Il RS deve predisporre una procedura per la condivisione delle informazioni relative agli attacchi subiti con il CSIRT Italia, ai sensi della Direttiva 1/8/2015 del Presidente del Consiglio dei ministri.
- **PLC-086 [media]**: Il RS deve individuare opportuni strumenti di monitoraggio per le piattaforme applicative sviluppate dall'Amministrazione della Giustizia per la cooperazione applicativa con altre PP.AA., in coerenza con il modello di interoperabilità previsto dal piano triennale ICT per la P.A. e dalle regole tecniche di sicurezza definite da AgID.
- **PLC-087 [media]**: RS deve predisporre delle procedure per il monitoraggio delle risorse a disposizione

dei sistemi al fine di verificare che esse siano adeguate a garantire la disponibilità dei servizi e dei dati. Il RSD deve verificare la corretta applicazione delle suddette procedure e deve predisporre regolari attività di monitoraggio sulle prestazioni dei sistemi presenti negli Uffici e nelle Sale Server di sua competenza al fine di gestire adeguatamente eventi, problemi e incidenti.

- **PLC-088 [alta]**: Il RS deve predisporre una suite di strumenti interni agli Uffici e alle Sale Server che permettano di monitorare regolarmente gli account del personale in modo da effettuare il log-off automatico degli utenti dopo un determinato tempo di inattività sulle macchine. Nel caso di utenze inattive per un lungo lasso di tempo, queste ultime devono essere segnalate al personale di amministrazione al fine di disabilitarle immediatamente. Gli strumenti devono essere in grado di tracciare in appositi log i tentativi falliti di accesso con utenze di amministrazione. Per le PdL con registrazione in ADN, quest'ultimo deve tenere traccia degli accessi riusciti e non riusciti.
- **PLC-089 [alta]**: Il RS deve definire i termini e le modalità di messa in opera di una Virtual Private Network (VPN) dalla RUG verso la rete esterna e viceversa, il cui controllo e monitoraggio spetta al RSD responsabile dell'Ufficio o Sala Server dove la VPN viene implementata. Il RSD deve mantenere traccia della VPN (compresa la rispettiva configurazione) in un apposito inventario e, periodicamente (almeno ogni tre mesi), deve valutare, di concerto con il RS, la reale necessità di mantenere attiva tale connessione.
- **PLC-090 [media]**: Il RS è tenuto a definire delle procedure operative per la verifica che le reti interne ad un Ufficio o una Sala Server siano classificate sulla base del livello di segretezza del dato trattato dai sistemi (workstation, server, PdL, NAS, ecc.) presenti nella rete o trasportato dalla stessa. Deve predisporre l'implementazione di meccanismi (hardware o software) di cifratura dell'informazione trasmessa da e verso reti interne classificate al più alto livello di segretezza, come pure l'utilizzo di dispositivi firewall, opportunamente configurati, per il controllo del traffico tra le diverse tipologie di rete.

6.2 Politiche e procedure di gestione dei log

Il RS deve definire delle misure di gestione dei log al fine di catturare eventi rilevanti per la sicurezza informatica dell'Amministrazione della Giustizia.

- **PLC-091 [alta]**: Il RSD deve verificare che all'interno degli Uffici e delle Sale Server di sua competenza vengano installati e configurati correttamente i software di Log Collector censiti dalla DGSIA. Inoltre, ha l'onere di controllare che gli amministratori dei Log Collector non siano amministratori dei sistemi dai quali i log sono generati, e deve moniotare che l'accesso al Log Collector è eseguito solo da personale ufficialmente autorizzato.
- **PLC-092 [alta]**: L'IS è tenuto a controllare che i dispositivi, ove previsto, siano configurati in modo da inviare tutti i suoi log a uno o più Log Collector installati all'interno della rete. Inoltre, deve verificare, ove sia di sua competenza, che i log registrati nel Log Collector non siano accessibili al personale non autorizzato alla loro visione e trattamento, e che il collegamento tra i sistemi locali dell'Ufficio o della Sala Server e il Log Collector deve avvenire mediante protocolli standard e sicuri, con mutua autenticazione delle parti. Infine, l'IS è tenuto a verificare che i dispositivi di sua diretta competenza e qualora gli stessi lo consentissero, siano configurati opportunamente per tracciare nei log i tentativi falliti di accesso con un'utenza di amministrazione. Qualora i dispositivi non lo consentano, l'IS lo segnala al RSD.
- **PLC-093 [media]**: RS stabilisce termini e modalità di svolgimento e controllo degli eventi rilevati

dagli strumenti firewall e IPS installati nella rete siano inviati ad un repository centrale per essere stabilmente archiviati con lo scopo di raccogliere, analizzare ed eventualmente distribuire indicatori di compromissione (IOC). Quanto sopra deve essere svolto al fine di verificare che vengano applicate le soglie, opportunamente definite per uno specifico Ufficio o Sala Server, sugli eventi da rilevare che, se superate, scatenano degli alert e riportano l'incidente al team di risposta agli incidenti.

- **PLC-094 [alta]**: Il RS deve predisporre un processo di logging che permetta di registrare tutte le informazioni utili a rilevare eventi di sicurezza informatica. Il RSD è responsabile della corretta implementazione del suddetto processo all'interno degli Uffici o Sale Server di sua competenza. Il processo di logging deve (i) identificare la natura e la durata della conservazione delle registrazioni cronologiche (log) relative agli eventi; (ii) individuare le registrazioni cronologiche necessarie a monitorare il funzionamento dei sistemi interni, definendo le modalità di archiviazione e durata della conservazione in modo da garantirne il loro utilizzo anche a fini giudiziari (investigazione su incidenti informatici). Il RS deve metter in piedi inoltre delle procedure operative di tracciamento nei log di tutte le azioni compiute da ogni utenza di amministrazione dei sistemi presenti nelle aree di sua competenza, inclusi l'aggiunta, la soppressione e l'aumento dei privilegi di specifiche utenze di amministrazione. Le registrazioni nei log devono comprendere riferimenti temporali attendibili e la descrizione dell'evento che le ha generate, devono essere adeguate al raggiungimento dello scopo di verifica per cui sono state previste e devono essere conservate per un periodo non inferiore a sei mesi. Il RS deve predisporre meccanismi di verifica che tutti i software applicativi degli Uffici e delle Sale Server siano conformi a tale processo. Infine, il RS deve predisporre dei meccanismi di controllo sull'esecuzione, con frequenza almeno bisettimanale, dell'analisi sui Log Collector che evidenzino eventuali anomalie nei log.
- **PLC-095 [media]**: Il RSD deve predisporre un processo, approvato dal RS, di verifica periodica, con cadenza almeno settimanale, che tutti i sistemi presenti negli Uffici o Sale Server di sua competenza, abbiano sufficiente spazio di storage per i log.
- **PLC-096 [media]**: Il RS, di concerto con il RSD interessato, deve definire le procedure di conservazione e di acquisizione delle registrazioni cronologiche a fronte di incidenti di sicurezza informatica, e la loro messa a disposizione all'Autorità Giudiziaria. Deve inoltre definire i requisiti necessari per la generazione dei log dei software applicativi, e deve verificare l'applicazione degli stessi da parte dei rispettivi fornitori. Infine, è tenuto a verificare che i log siano archiviati e firmati digitalmente su base periodica.

7 DISASTER RECOVERY E CONTINUITÀ OPERATIVA

Il RS definisce il piano di Disaster Recovery e Continuità Operativa e descrive le sue modalità di attuazione e gestione.

7.1 Continuità Operativa

L'Agenzia per l'Italia Digitale definisce la Continuità Operativa nel contesto ICT come la capacità di un'organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento a eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e delle funzioni istituzionali (Circolare AgID, Linee guida per il disaster recovery delle pubbliche amministrazioni. Aggiornamento 2013[1]).

- **PLC-097 [media]**: Il RS deve redigere un piano di continuità operativa di ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza in collaborazione con i RSD. Il piano deve tener conto dei livelli di servizio erogati, dei periodi di criticità e presidio, i relativi tempi di ripristino e gli obiettivi temporali di back-up e deve individuare l'infrastruttura di rete a supporto della continuità operativa dell'Ufficio o Sala Server di riferimento. Deve essere implementato inoltre un processo di verifica periodica del piano di continuità operativa.
- **PLC-098 [media]**: Il RS deve controllare che i sistemi installati negli Uffici e Sale Server di sua competenza siano progettati e messi in opera con diversi stati funzionali predefiniti, di modo da garantirne la disponibilità in situazioni critiche, quali sotto attacco e durante un ripristino.

7.2 Ridondanza geografica

Nel formulare il piano di Disaster Recovery, l'RS, di concerto con ogni RSD per la rispettiva competenza territoriale, individua idonee forme di ridondanza geografica dei sistemi informativi, installati negli Ufficio o Sale Server, che consentano di superare crisi determinate da eventi catastrofici naturali o di origine umana.

- **PLC-099 [bassa]**: Il RS, in collaborazione con i RSD, deve definire un piano di messa in protezione contro le calamità naturali, attacchi o incidenti fisici degli Uffici e delle Sale Server di sua competenza. Per ognuno di essi, il RS, in accordo con i RSD, deve individuare la rispettiva ridondanza geografica.

7.3 Disaster recovery

Il RS, di concerto con i RSD, ognuno per la rispettiva competenza territoriale, individua e documenta le condizioni per l'attivazione dello stato di emergenza informatica e le strutture preposte alla sua gestione.

- **PLC-100 [media]**: Il RS, in collaborazione con i RSD, deve redigere un piano di disaster recovery per ogni Ufficio Centrale, Ufficio Giudiziario e Sala Server di sua competenza. Il RS deve inoltre implementare un processo di verifica periodica del piano di disaster recovery. Il piano deve specificare le strutture preposte alla gestione e le procedure relative alle fasi di: reazione all'emergenza, gestione dell'emergenza, riattivazione dei servizi e ritorno alla normalità. Il piano di disaster recovery deve individuare un team di risposta agli incidenti con i rispettivi ruoli e responsabilità. Il RS deve definire inoltre le procedure che consentono (i) di istruire il personale interno sulle modalità di acquisizione dell'informazione relativa agli incidenti di sicurezza informatica che deve essere comunicata ai responsabili del team di risposta, e (ii) il coordinamento tra le parti interessate all'incidente. Per il coordinamento, il team di risposta deve informare il RS. Quest'ultimo informerà i rappresentanti

[1] http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf

dell'Autorità Giudiziaria qualora si verificassero eventi configurabili come fatti di reato (es. accessi abusivi al sistema), riportando a essi ogni circostanza utile ai fini della corretta informazione. Il RSD deve applicare il piano di risposta agli incidenti in maniera tempestiva in modo da contenerne l'impatto e/o la mitigazione degli effetti. Il RS, in accordo con il RSD, deve definire i criteri e le modalità di aggiornamento del piano di risposta agli incidenti, in considerazione anche delle esperienze passate.

- **PLC-101 [media]**: Il RSD deve supervisionare l'operato del team locale di risposta agli incidenti dell'Ufficio o della Sala Server di sua competenza. Il team di risposta deve utilizzare un sistema SIEM, censito da DGSIA, per la rilevazione degli eventi di sicurezza informatica interni ai contesti di sua competenza, e deve essere in grado di valutarne gli impatti. I metodi di identificazione, collezione e acquisizione delle informazioni (utilizzate anche come evidenze di un attacco) relativi a eventi di sicurezza devono essere ufficializzati al team di risposta mediante opportune procedure. Gli incidenti devono essere analizzati e classificati dal team di risposta al fine di aggiornare e migliorare il piano di risposta. Il team di risposta deve individuare e identificare la radice della causa dell'incidente nella maniera più accurata e dettagliata possibile, determinando la strategia di contenimento più efficace.

- **PLC-102 [media]**: Il piano di disaster recovery, redatto dal RS di concerto con il RSD, deve prevedere un piano di ripristino specifico per gli incidenti di sicurezza informatica, individuando un team di ripristino con i rispettivi ruoli e responsabilità. Il piano di ripristino deve tenere in considerazione almeno:
    - I livelli di servizio stabiliti all'interno dell'Ufficio Centrale, Ufficio Giudiziario e Sala Server, come ad esempio, percentuale di disponibilità, tempi di inattività massimi consentiti, offerta di larghezza di banda garantita ecc. In questa categoria devono essere considerati anche eventuali ingaggi esterni di personale qualificato previsti da contratti in essere da affiancare al team di ripristino per eventi di sicurezza informatica di una certa rilevanza.
    - I nomi di due o più membri del personale di gestione ufficialmente autorizzati con le relative informazioni di contatto (es., numero di telefono, indirizzo e-mail, ecc.) che devono essere contattati per attivare il piano.
    - Le informazioni di contatto (es., numero di telefono, indirizzo e-mail, ecc.) delle persone del team di ripristino che sono in grado di attuare il piano in quanto istruite e preparate.

    Il piano di ripristino deve inoltre delineare con accuratezza la guida di ripristino, riportando l'ordine preciso in cui i sistemi devono essere rimessi in operatività. Devono essere ben identificate le fasi principali del ripristino includendo, per ognuna di esse, le procedure e i processi da eseguire, i criteri di uscita da ogni fase e le notifiche alle principali parti interessate. Devono inoltre essere definiti i criteri e le modalità di aggiornamento del piano di ripristino agli incidenti, in considerazione anche delle esperienze passate, attraverso la definizione di processi di verifica delle funzionalità di ripristino che mirino a garantire che le tecnologie e i processi messi in atto e le persone coinvolte nella fase di ripristino permettano di ristabilire l'operatività dell'Ufficio o della Sala Server in tempi accettabili e in modo efficace.

- **PLC-103 [media]**: L'IS deve controllare e supervisionare che i sistemi in esercizio compromessi vengano ripristinati usando la configurazione standard.

- **PLC-104 [bassa]**: Il personale del team di ripristino che esegue le operazioni di recupero da un incidente deve produrre un report dettagliato in cui vengono documentate le attività eseguite. Tale

report deve essere visionato dal RSD dell'Ufficio o Sala Server coinvolti nell'incidente, e dev'essere approvato dal RS.

- **PLC-105 [bassa]**: Il RS deve impartite a tutti i RSD le procedure ufficiali per la gestione delle pubbliche relazioni a seguito di un incidente di sicurezza informatica.

7.4 Gestione degli incidenti

La storia recente degli incidenti vissuti da altre istituzioni ed organizzazioni pubbliche e private costituisce un elemento di contesto che deve essere attentamente considerato nella definizione delle politiche di gestione degli incidenti.

Alla luce di un numero sempre crescente di eventi di sicurezza informatica, è fondamentale che i processi di gestione dei rischi includano la definizione e la gestione di un piano globale di risposta e ripristino dagli incidenti di sicurezza informatica (Cyber Incident Response Plan - CIRP) che è parte integrante del piano di continuità operativa (Business Continuity Plan - BCP). Il CIRP corrisponde a un insieme di documenti che individuano una serie di procedure per affrontare attacchi informatici contro i sistemi interni dell'Amministrazione della Giustizia (Rif.[**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**,**Errore. L'origine riferimento non è stata trovata.**]).

L'identificazione e la priorità delle risorse, ad esempio, è fondamentale nel definire piani di risposta e ripristino più efficaci, e scenari di test realistici, consentendo una più rapida ripresa dagli incidenti, e quindi riducendo al minimo l'impatto degli stessi. Inoltre, un miglioramento continuo dei piani attraverso le lezioni apprese dagli eventi passati, inclusi quelli di altre organizzazioni, può contribuire a garantire la continuità operativa dei servizi critici.

Il processo di gestione degli incidenti si articola nelle seguenti macro fasi:

- Rilevazione/identificazione/classificazione – vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell'Amministrazione.
- Contenimento – vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione.
- Eliminazione – vengono eliminate le cause che hanno portato al verificarsi dell'incidente.
- Ripristino – vengono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento.
- Follow-up – viene verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Ai fini della definizione delle politiche di sicurezza, si è tenuto conto degli incidenti registrati dalla DGSIA nell'ultimo triennio, delle modalità di azione via via perfezionatesi sia con riferimento alle strutture interne che ai fornitori esterni.

7.5 Team di risposta/ripristino agli incidenti

Il RS, al fine di un'adeguata gestione in risposta agli incidenti, incarica un apposito team perché riceva le segnalazioni degli incidenti che dovranno essere gestiti secondo le procedure operative indicate nel documento dedicato adottato dal RS su proposta del RSD.

Per l'Amministrazione della Giustizia, data la sua peculiarità di dispiegamento capillare sull'intero territorio italiano, è previsto un modello distribuito del team di risposta. Si prevedono più team di risposta distribuiti sul territorio: in prima istanza, un team per ognuno degli uffici dirigenziali di coordinamento territoriale CISIA. Per il coordinamento dei diversi team di risposta dispiegati sul territorio, è previsto un team di risposta di coordinamento centrale, presso la DGSIA, che ha il compito di ricevere centralmente le segnalazioni di incidenti di sicurezza, e coordinare le risposte agli incidenti, ridistribuendo specifici compiti ai team distribuiti e coinvolti per la risoluzione dell'incidente, in modo che il processo di risposta sia coerente in tutta l'Amministrazione della Giustizia e le informazioni siano condivise tra i team in maniera coordinata.

Per la composizione dei team di risposta, si rimanda al documento da approvare e da adottarsi entro trenta giorni dall'adozione del presente.

8 POLITICHE DI GOVERNO E GESTIONE DELLA SICUREZZA

Il RS, nell'espletamento delle sue funzioni, deve mettere in opera delle politiche e delle procedure atte a disciplinare il governo della sicurezza e la gestione del rischio a cui l'Amministrazione della Giustizia è esposta, con particolare attenzione alla gestione del rischio derivante dalla fornitura di servizi e sistemi informatici da parte di fornitori e consulenti esterni.

8.1 Governance della Sicurezza Informatica

A supporto dell'intero processo di gestione della sicurezza informatica dell'Amministrazione della Giustizia, è prevista la costituzione, presso la DGSIA, di un *Tavolo permanente per la governance della sicurezza informatica* (TGSI) con il mandato, tra altro, di fornire informazioni e assistenza al personale del Ministero della Giustizia e ai magistrati operanti negli Uffici Giudiziari, per l'attuazione (i) di misure proattive volte a ridurre i rischi di incidenti di sicurezza informatica e (ii) di misure reattive agli eventuali incidenti in corso.

Il Tavolo, quindi, si propone di assicurare una governance centrale delle politiche di attuazione del presente piano, attraverso:

- un coordinamento centralizzato e un punto unico di contatto per tutte le questioni inerenti la sicurezza ICT, che ha una visione d'insieme di quanto avviene nell'Amministrazione;
- gestione centralizzata degli incidenti tramite il ricorso a personale specializzato, pur rimandando l'attività operativa al personale preposto per la gestione degli incidenti (SOC-giustizia);
- il continuo aggiornamento sugli sviluppi nel campo della sicurezza, con il contributo dell'Ufficio per il coordinamento delle sale server e la sicurezza informatica;
- la cooperazione della propria comunità di riferimento, sensibilizzandola sui temi della sicurezza (awareness);
- instaurando una costante interlocuzione con il CSIRT Italia, per contribuire alla crescita della collaborazione e condivisione tra le pubbliche amministrazioni.

La funzione del Tavolo è sostanzialmente interna, avendo come comunità di riferimento il personale del Ministero della Giustizia e l'Autorità Giudiziaria, almeno per quanto attiene all'utilizzo dei servizi e delle infrastrutture. Il Tavolo è pensato come organo consultivo, propositivo e di controllo, che opera in stretto contatto con la gestione operativa dei sistemi informatici e con gli incaricati al trattamento dell'incidente (team di risposta e team di ripristino dell'incidente), presenti nel SOC-giustizia con unità operative dispiegate nel territorio.

Il Tavolo ha la funzione di promuovere la prevenzione degli eventi dannosi, facendosi portatore di iniziative atte a determinare un aumento del livello di sicurezza.

In sintesi, le funzioni primarie che si prevedono per il Tavolo permanente, meglio dettagliate nel dedicato documento eventualmente da adottarsi con separato atto, sono:

- Security governance,
- Security Strategy,
- Security Service Management,
- Security Risk Management,

- Security Program & Project Management.

Per svolgere le funzioni di cui sopra, è indispensabile avere una conoscenza approfondita e aggiornata dell'infrastruttura, cioè di reti, server, PdL e software in uso, mediante un censimento iniziale degli asset stessi in un sistema di asset inventory e la registrazione di ogni successiva variazione (dismissioni, aggiornamenti, acquisizioni). È altresì indispensabile la collaborazione con i fornitori per le soluzioni prodotte e mantenute da terzi, stipulando contratti che cautelino l'Amministrazione della Giustizia rispetto all'aggiornamento del software e del middleware, vincolando il fornitore a seguire linee evolutive che evitino di avere in produzione prodotti non aggiornabili.

È necessario che il Tavolo provveda a:

- Attivare delle unità operative a supporto della sicurezza affinché recepiscano le segnalazioni di vulnerabilità, traducendole in azioni preventive sui sistemi e sulle postazioni di lavoro, eventualmente contattando i fornitori di servizi e stabilendo un ordine di priorità alle azioni da intraprendere sulla base della rilevanza delle informazioni da proteggere e del servizio e del danno che ne deriverebbe.
- Controllare che le azioni preventive si concludano in un tempo consono alla rilevanza della segnalazione stessa e alla gravità della minaccia. Nel caso, invece, la segnalazione non fosse preventiva ma reattiva rispetto a un incidente (es. un'intrusione o un malware), il Tavolo nulla attiva, essendo di competenza del SOC-giustizia.

A queste funzioni di base il Tavolo provvede ad attivare altri servizi che incrementano la sicurezza globale come l'attenzione all'utente finale e alla sua consapevolezza, la formazione, la valutazione dei prodotti o dei progetti.

Il Tavolo è l'organo che disciplina in modo rigoroso gli aspetti salienti della sicurezza informatica dell'Amministrazione della Giustizia, definendone politiche, procedure e processi a supporto. Il RS è quindi posto al vertice di tale struttura, a cui spetta la definizione dell'assetto organizzativo interno, come: la definizione dei ruoli e delle responsabilità per la sua operatività; le unità operative centrali (presenti nella DGSIA) e quelle distribuite sul territorio (con riferimento all'attuale suddivisione territoriale già applicata per i CISIA) preposte alla gestione operativa della sicurezza (es., team di coordinamento della gestione di un incidente, team di risposta, team di ripristino, ecc.); gli amministratori di sistema specializzati nella sicurezza informatica; gli incaricati al trattamento del dato per operazioni di back-up, conservazione (es. dei log applicativi) e distruzione; team di ricezione delle segnalazioni degli incidenti dagli Uffici Giudiziari e ministeriali.

Il Tavolo può prevedere la partecipazione di personale esterno all'Amministrazione e/o di rappresentanti degli Uffici Giudiziari in veste di consulente per quanto di competenza specifica. Gli incarichi dovranno essere debitamente formalizzati mediante lettere di incarico protocollate, e gli incaricati dovranno accettare esplicitamente l'investitura, impegnandosi a contribuire attivamente al corretto espletamento della funzione prevista per il Tavolo permanente.

Il suddetto Tavolo dovrà essere costituito almeno da:

- Direttore Generale pro tempore, in qualità di RS;
- Dirigenti pro tempore dei CISIA territorialmente di riferimento per le sale server nazionali: Milano, Napoli, Palermo e Roma, in qualità di RSD;
- Dirigente pro tempore dell'Ufficio per il coordinamento delle sale server e la sicurezza informatica;

- Dirigente pro tempore dell'Ufficio per le reti, la connettività e l'interoperabilità;
- Dirigente pro tempore dell'Ufficio per l'attuazione della trasformazione digitale.

Il Tavolo permanente ha anche la funzione di collettore degli eventi, per mantenere un controllo centrale e diffondere a tutti i livelli la conoscenza sulle iniziative in essere nell'ambito della sicurezza, assicurandone anche il coordinamento a livello locale.

8.2 Politica di gestione dei ruoli e delle responsabilità della sicurezza

Il RS deve definire e rendere noti i ruoli e le responsabilità inerenti la sicurezza informatica a tutto il personale e alle terze parti rilevanti per l'Amministrazione della Giustizia, cioè fornitori, consulenti e utenti.

- **PLC-106 [alta]**: Il RS deve identificare i ruoli e le responsabilità inerenti la sicurezza informatica, nonché le attività in carico a ciascun ruolo.
- **PLC-107 [alta]**: Il RS deve definire le regole di sicurezza che disciplinano l'utilizzo e il trattamento delle informazioni e degli strumenti informatici da parte di tutto il personale.
- **PLC-108 [alta]**: Il RS deve definire le regole di sicurezza che disciplinano l'utilizzo e il trattamento delle informazioni e degli strumenti informatici da parte di terze parti (fornitori, consulenti, utenti).

8.3 Politica di gestione requisiti di resilienza a supporto della fornitura di servizi critici

Il RS deve definire e rendere noti i requisiti di resilienza a supporto della fornitura di servizi critici per l'Amministrazione della Giustizia.

- **PLC-109 [bassa]**: Il RS, con l'ausilio dei RSD, deve redigere e gestire un elenco dei servizi critici rispetto ai fattori di confidenzialità, integrità e disponibilità, e dei rispettivi requisiti di resilienza che gli Uffici e le Sale Server erogano a tutti coloro che ne fanno uso.

8.4 Politica di gestione della sicurezza delle informazioni

Il RS deve definire le politiche di sicurezza delle informazioni applicate all'interno dell'Amministrazione della Giustizia, e identificare i ruoli e le responsabilità inerenti la sicurezza delle informazioni.

- **PLC-110 [alta]**: Il RS deve verificare che la gestione informatica del dato e delle informazioni deve essere coerente con la normativa di settore vigente in materia di sicurezza informatica, per la parte relativa al trattamento di dati giudiziari.
- **PLC-111 [media]**: Il RS deve verificare che venga identificato il responsabile del trattamento del dato e delle informazioni di ogni Ufficio Centrale e Ufficio Giudiziario.
- **PLC-112 [media]**: Il RS deve verificare che venga identificato il responsabile della conservazione delle informazioni (dati e documenti) di ogni Ufficio Centrale e Ufficio Giudiziario.
- **PLC-113 [media]**: Il RS, di concerto con i RSD, deve redigere un piano della sicurezza per il sistema di conservazione adottato all'interno degli Uffici e delle Sale Server di sua competenza.
- **PLC-114 [media]**: Il RS, di concerto con i RSD, deve verificare che il processo di conservazione dei documenti informatici adottato all'interno degli Uffici e delle Sale Server di sua competenza deve essere conforme alla normativa di settore.

- **PLC-115 [bassa]**: Il RS, con l'ausilio dei RSD, deve verificare che ogni struttura identificata come P.A. di sua competenza abbia compilato e firmato digitalmente con marca temporale il Modulo di implementazione delle misure minime di sicurezza per le pubbliche amministrazioni, se dovuto.

- **PLC-116 [alta]**: Il RS deve redigere un codice deontologico in materia di sicurezza informatica che deve essere sottoscritto dal personale interno degli Uffici e delle Sale Server dell'Amministrazione della Giustizia.

8.5 Politica di gestione dei requisiti legali in materia di sicurezza informatica

Il RS deve identificare i requisiti e gli obblighi legali riguardanti la privacy e le libertà civili che l'Amministrazione della Giustizia deve rispettare.

- **PLC-117 [bassa]**: Il RS deve individuare tutti i requisiti e gli obblighi legali riguardanti la privacy inerenti la sicurezza informatica, con particolare riguardo all'art. 25 del D.Lgs 51 del 2018. Tali requisiti e obblighi devono essere formalizzati in un documento ufficiale che disciplina anche la procedura per la comunicazione degli stessi alle parti interessate, cioè personale degli Uffici e delle Sale Server, fornitori e consulenti dell'Amministrazione della Giustizia,

8.6 Politica di gestione del rischio di sicurezza informatica

Il RS, relativamente alla consapevolezza del rischio di sicurezza informatica a cui si è esposti durante l'operatività, deve: (i) individuare e gestire le minacce e le vulnerabilità a cui è esposta l'Amministrazione della Giustizia e (ii) individuare i potenziali impatti che tali minacce e vulnerabilità hanno sulla sua operatività. Il RS è responsabile anche di definire i processi di gestione del rischio di sicurezza informatica derivante dalla catena di approvvigionamento dei sistemi e dei servizi informatici a supporto della sua operatività. Il RS è tenuto inoltre a definire e priorizzare le risposte al rischio.

- **PLC-118 [media]**: Il RS, di concerto con i RSD, deve predisporre un piano di ricerca e gestione delle vulnerabilità per ogni Ufficio e Sala Server, che regoli le modalità con cui tali ricerche devono essere eseguite, identifichi gli eventi che scatenano tali ricerche e gli intervalli di tempo di ripetizione delle suddette, e priorizzi le vulnerabilità trovate.

- **PLC-119 [bassa]**: Il RS è tenuto a mantenere un inventario delle vulnerabilità conosciute all'interno di ogni Sala Server e Ufficio di sua competenza, organizzato per tipologia di risorsa (sistema, dispositivo, applicativo, ecc.). Tali vulnerabilità devono essere identificate mediante un codice univoco e opportunamente documentate.

- **PLC-120 [alta]**: Il RS deve predisporre un centro di riferimento interno all'Amministrazione della Giustizia per la raccolta delle informazioni inerenti minacce e vulnerabilità di sicurezza informatica, e la tenuta di un elenco ufficiale delle fonti esterne attendibili e fidate per la raccolta delle informazioni inerenti minacce e vulnerabilità di sicurezza informatica.

- **PLC-121 [bassa]**: Il RS, con supporto dei RSD, deve definire, per ogni Ufficio e Sala Server, un processo regolare di analisi di impatto delle vulnerabilità e delle minacce sulla rispettiva operatività. Il RS deve inoltre nominare un responsabile della gestione di tale processo.

- **PLC-122 [alta]**: Il RSD deve determinare il rischio di sicurezza informatica a cui le Sale Server di sua competenza sono esposte. Tale rischio deve essere comunicato al RS. Nel determinare tale rischio il

RSD deve tener conto delle minacce e delle relative probabilità di accadimento, della tipologia degli apparati e dei dispositivi coinvolti (PC, workstation, Server, switch, router, ecc.), del livello di gravità delle vulnerabilità e del loro potenziale impatto sull'operatività. Inoltre il RSD, di concerto con il RS, deve redigere un piano di gestione dei rischi. Il RS può valutare la fornitura di software idoneo alle attività di cui sopra. Relativamente agli Uffici, qualora il RSD avesse cognizione dei rischi di sicurezza informatica a cui gli stessi sono esposti, lo stesso è tenuto a comunicarlo al RS per eventuali disposizioni di competenza.

- **PLC-123 [bassa]**: Il RS definisce opportuni processi di gestione del rischio applicabile a ogni Ufficio e Sala Server, stabilendo attività, ruoli, responsabilità, modalità di gestione e controllo. Questi processi devono essere concordati con i vertici istituzionali dell'Amministrazione della Giustizia.

- **PLC-124 [media]**: Il RS deve opportunamente valutare ed eventualmente documentare il rischio di sicurezza informatica associato alla fornitura di sistemi e servizi esterni per ogni Ufficio e Sala Server dell'Amministrazione della Giustizia.

Il RS adotta, laddove necessario per gli Uffici Giudiziari, ulteriori policy, al fine dell'innalzamento del livello complessivo di sicurezza.

- **PLC-125 [alta]**: Il RS deve far sì che nei contratti di fornitura dei sistemi e dei servizi sottoscritti dai fornitori sia prevista la conformità alle misure minime di sicurezza informatica, previste dal piano della sicurezza dell'Amministrazione della Giustizia.

- **PLC-126 [media]**: Il RS deve predisporre una serie di iniziative a supporto del monitoraggio dei fornitori sulla base della tipologia del sistema e/o servizio fornito e/o erogato, e sulle attività e gli obblighi contrattuali sottoscritti dagli stessi.

- **PLC-127 [media]**: Il RS, di concerto con i RSD, deve definire e verificare i piani di risposta e ripristino da incidenti di sicurezza informatica, in cooperazione e coordinamento con i fornitori dei sistemi e dei servizi ritenuti ad alta criticità per l'Ufficio o la Sala Server in questione.

8.7 Politica di produzione, diffusione e gestione della documentazione di sicurezza

Il RS definisce le procedure di gestione della documentazione di sicurezza, che riguardano le attività riferite all'acquisizione, produzione, archiviazione e la loro diffusione tra le diverse funzioni.

Il RS deve individuare gli strumenti informatici e definire le rispettive procedure operative a supporto della gestione e della divulgazione della documentazione di sicurezza, individuando i mezzi e le modalità sicure di comunicazione alle figure interessate dell'avvenuta pubblicazione di nuovi documenti, della revisione di documenti esistenti o della loro revoca.

8.8 Politica di formazione del personale

Uno degli obiettivi di fondamentale importanza per il RS è di sviluppare una corretta cultura della sicurezza in tutto il personale dell'Amministrazione della Giustizia, indipendentemente dalle sue responsabilità. Tutto il personale deve avere quindi una consapevolezza dei rischi e della propria capacità di prevenire incidenti e/o di gestirli.

A tal proposito, il RS ha l'obbligo di definire un piano di formazione e aggiornamento del personale dell'Amministrazione della Giustizia, ai fini della corretta gestione della sicurezza informatica, definendo appropriati livelli e contenuti per:

- il personale dirigenziale su specifiche tematiche di gestione del rischio associato alla sicurezza informatica e il personale DGSIA degli Uffici dirigenziali centrali.
- i soggetti specificamente preposti alla gestione della sicurezza informatica, come ad esempio i dirigenti CISIA o i funzionari dispiegati sul territorio;
- i tecnici informatici come il personale che operativamente tratta la sicurezza fisica dei sistemi e dei dati, o il personale di amministrazione dei sistemi, dei dispositivi e delle reti;
- gli utenti finali dei sistemi applicativi dell'Amministrazione della Giustizia.

La formazione del personale dei quadri dirigenziali è fondamentale e dovrà essere costantemente aggiornata sui nuovi paradigmi di sicurezza e sulle normative vigenti.

Il personale DGSIA presente negli Uffici centrali e coinvolto: (i) nello sviluppo e nella manutenzione dei sistemi applicativi; (ii) nella gestione dell'infrastruttura tecnologica e di rete; (iii) nella selezione e nell'acquisto di tecnologie a supporto della sicurezza informatica e (iv) nella definizione dei contratti con i fornitori dell'Amministrazione della Giustizia, dovrà essere formato su problematiche di sicurezza strettamente collegate al rispettivo perimetro di competenza.

I soggetti specificatamente preposti alla gestione della sicurezza informatica devono essere istruiti sull'organizzazione interna, comprendono le figure come i dirigenti CISIA e i funzionari dispiegati sul territorio presso gli Uffici o le Sale Server. Essi devono essere formati sulle politiche interne di gestione della sicurezza, in modo da verificare che le stesse siano ben comprese dal personale interno ma soprattutto dai fornitori e consulenti esterni, per una loro corretta attuazione.

I tecnici informatici rappresentano coloro che applicano o supervisionano i passi delle procedure definiti nei loro contesti di competenza. È il personale che operativamente tratta la sicurezza fisica dei sistemi e dei dati, o amministra sistemi, dispositivi e reti. Essi devono essere continuamente aggiornati sui nuovi prodotti acquisiti dal Ministero, su eventuali alert nonché sulle nuove minacce, in modo che siano in grado anche di analizzare le situazioni e verificare che i passi delle procedure siano stati applicati correttamente. Una volta analizzata la situazione, hanno il compito di riferirla ai soggetti specificamente preposti alla gestione della sicurezza informatica che a loro volta la riporteranno ai vertici dirigenziali.

La formazione agli utenti finali è la chiave per rendere quest'ultimi consapevoli del rischio di sicurezza a cui sono esposti durante l'operatività quotidiana e di conseguenza consente di evitare la maggior parte degli incidenti. Quasi tutti gli incidenti più importanti riportati dalle cronache sono stati causati da pratiche errate o semplici errori degli utenti, come apertura di allegati e-mail sospetti o installazione di software non autorizzato. Altri esempi sono legati a una non attenta navigazione sul web, che a volte può portare a selezionare banner pubblicitari ingannevoli e quindi a eseguire codice malevolo. Da non sottovalutare la pratica dello *spear phishing* che, a differenza del phishing generico, è concepito per risultare più rilevante per il contesto sociale-lavorativo di una specifica vittima, la quale riceve tipicamente una sollecitazione verso un link o un file attraverso e-mail apparentemente provenienti da persone conosciute o via messaggi istantanei, strumenti la cui popolarità è in forte aumento. Gli esempi di incidenti basati sulla carenza di cultura digitale sono innumerevoli.

Per questo motivo uno degli obiettivi del RS è di creare, attraverso una specifica formazione, un insieme di buone pratiche su comportamenti errati da evitare, evidenziando le conseguenze che potrebbero ripercuotersi non solo sulla singola postazione di lavoro, bensì sull'intera struttura / infrastruttura. Per tali utenti devono essere definiti dei corsi di formazione ad hoc e tecnologicamente avanzati sul corretto utilizzo di strumenti informatici messi a disposizione, come ad esempio la formazione sull'utilizzo di tecniche di cifratura dei dati contenuti sui dispositivi interni o rimovibili.

Affinché tali programmi di formazione risultino essere adeguati, essi dovranno essere somministrati al

personale di riferimento in maniera cadenzata, annuale per gli utenti finali, più serrata per le altre figure. Rimane inteso che tale cadenza potrà essere rivista e aggiornata a seguito di particolari eventi o situazioni specifiche.

8.9 Politica di regole comportamentali dei fornitori

Il RS è tenuto a definire le politiche e le procedure che disciplinano le attività e i comportamenti dei fornitori, in materia di sicurezza informatica.

- **PLC-128 [alta]**: Il RS è tenuto a verificare che tutte le attività di studio e di analisi dei sistemi informativi esistenti e delle collegate infrastrutture tecnologiche, individuazione delle vulnerabilità, progettazione dell'architettura di sicurezza e definizione delle regole e procedure di sicurezza, espletate da un fornitore presso gli Uffici o le Sale Server di sua competenza, siano condotte in modo da assicurare un elevatissimo livello di riservatezza, al fine di preservare la segretezza delle informazioni gestite dai sistemi informativi dell'Amministrazione della Giustizia, nonché gli strumenti informatici utilizzati per la gestione di tali informazioni.

- **PLC-129 [alta]**: Il RS deve controllare che il fornitore predisponga una serie di misure di carattere amministrativo volte a:
  - mantenere riservate le architetture e le scelte tecniche di dettaglio (hardware impiegato, sistemi operativi, configurazione etc.) di tutti i sistemi dell'Amministrazione della Giustizia, specialmente quelle relativa all'area del penale;
  - evitare in modo assoluto la circolazione di qualunque informazione relativa alle vulnerabilità dei sistemi, o a qualunque debolezza dell'organizzazione, che possa essere utilizzata per potenziali attacchi (tali informazioni devono essere fornite esclusivamente ai committenti dell'attività tramite canali riservati);
  - mantenere segrete le informazioni in merito alle misure adottate - o da adottare - per eliminare o mitigare le vulnerabilità;
  - coinvolgere personale di provata lealtà, che goda della piena fiducia dell'Amministrazione.

- **PLC-130 [alta]**: Il RS deve adottare idonee iniziative affinché tutta la documentazione, in formato elettronico o cartaceo, rilasciata dal fornitore, deve essere gestita in modo da assicurare la riservatezza dei contenuti. I documenti (sia cartacei che digitali) devono tutti essere opportunamente identificati:
  - se in bozza, con la dicitura bozza in filigrana;
  - quando protocollato, tramite il barcode del protocollo sulla prima pagina e la segnatura su tutte le altre pagine, sia che si tratti di documento acquisito dal protocollo come principale sia come allegato.
  - se è documentazione di progetto (manuali, progetto et alia) siano privi in ogni parte di loghi aziendali e corredati da intestazioni ministeriale.

  Per quanto concerne la documentazione sia su carta che digitale vale quanto previsto all'allegato "Regole per la gestione documentale relativa ai procedimenti sottoposti a particolari misure di sicurezza".

9 VERIFICA DELLA CONFORMITÀ E MIGLIORAMENTO DELLA SICUREZZA

9.1 Manutenzione delle politiche, delle procedure e dei processi

Il Piano della Sicurezza è un documento "vivo", per cui è soggetto a revisione periodica con possibili aggiornamenti delle politiche, delle procedure e dei processi ivi elencati. L'aggiornamento del Piano, a opera del RS, può avvenire per:

- Evoluzione tecnologica e relativa obsolescenza, degli apparati, dei sistemi e dei dispositivi preposti alla sicurezza informatica e presenti nell'Amministrazione della Giustizia.
- Variazione della normativa cogente, attraverso l'emanazione di nuove leggi e/o l'abrogazione di altre che impattano direttamente o indirettamente sulla sicurezza informatica dell'Amministrazione della Giustizia.
- Esperienze operative rilevate nell'ambito delle attività di audit interne o lezioni apprese da incidenti di sicurezza accaduti che evidenziano l'inadeguatezza o l'incompletezza delle politiche, delle procedure o dei processi per particolari aspetti della sicurezza informatica dell'Amministrazione della Giustizia.

9.2 Politiche e procedure di verifica e miglioramento (auditing)

Il RS ha l'obbligo di pianificare, con periodicità almeno annuale, audit interni del sistema di gestione della sicurezza per verificare se le politiche, le procedure e i processi a supporto della sicurezza informatica siano efficacemente attuate.

Il RS deve mantenere un'analisi aggiornata, attraverso specifiche attività di audit, del rischio informatico a cui l'Amministrazione della Giustizia è esposta, aggiornando opportunamente la stima delle criticità associate e rivalutando la strategia di gestione del rischio (eliminazione, trasferimento, mitigazione, accettazione), modificandola opportunamente qualora necessario.

- **PLC-131 [bassa]**: Il RS predispone un piano di misurazione dell'efficacia sul medio e lungo termine delle contromisure adoperate al fine di affinare, eliminare o inserire nuovi rischi e di migliorare i processi di protezione dei dati e dei sistemi. Il RS deve definire inoltre le procedure di assessment periodiche, relativamente all'analisi dell'efficacia delle tecnologie e dei processi adottati a protezione dei dati e dei sistemi. Tali attività devono essere eseguite in collaborazione con esperti nazionali e internazionali in materia di protezione e sicurezza dei dati e dei sistemi.

10 TABELLA DI CONFORMITÀ AL D.Lgs 51/2018

La seguente tabella riporta la corrispondenza tra le politiche di sicurezza individuate e le disposizioni di cui all'art. 25 del D.lgs. n. 51/2018

Disposizioni di cui all'art. 25 del D.lgs. n. 51/2018	**Politiche corrispondenti**
a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);	**PLC-013, PLC-014, PLC-015**, PLC-016, **PLC-108**
b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);	PLC-037, **PLC-041**, **PLC-046**, PLC-063, **PLC-073**
c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);	**PLC-017**, **PLC-018**, **PLC-024**, **PLC-027**, PLC-024
d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);	**PLC-020**, **PLC-021**, PLC-022, **PLC-024**
e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);	PLC-026, **PLC-027**, PLC-028, **PLC-035**, PLC-036
f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);	**PLC-066**, **PLC-069**, **PLC-079**, **PLC-088**
g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);	**PLC-029**, **PLC-091**, **PLC-092**, **PLC-094**
h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);	**PLC-031**, **PLC-032**, PLC-033, PLC-034
i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);	**PLC-059**, PLC-060, **PLC-061**, PLC-097, PLC-098
l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).	PLC-062, **PLC-064**, **PLC-065**, **PLC-120**, PLC-127

11 ELENCO DELLE PROCEDURE DI SICUREZZA

Id	Ambito	Descrizione sintetica	Nome della procedura	Policy
Proc-01	Gestione Hardware e Infrastruttura di rete	La procedura consente di mappare i processi di gestione, individuati dal framework ITIL 2011, sulla tassonomia delle funzioni FCAPS dello standard ISO 7498-4. La risultante matrice permette di mettere in corrispondenza i processi di gestione previsti per l'Amministrazione della Giustizia con i nodi della rete e i sistemi di ICT Management, al fine di poter mettere sotto controllo e sotto monitoraggio PdL, workstation, server e qualsiasi dispositivo o appliance presente nella rete di un Ufficio o Sala Server.	Gestione dei nodi di una rete interna ad un Ufficio o Sala Server.	PLC-001
Proc-02	Gestione degli incidenti	Procedura che consente di definire il flusso di lavoro previsto per la divulgazione interna di segnalazione, avvisi e annunci mediante: 1. Raccolta delle informazioni da fonti esterne. 2. Valutazione della pertinenza e della fonte delle informazioni. 3. Valutazione del rischio sulla base delle informazioni raccolte e analizzate. 4. Distribuzione delle informazioni.	Procedura di divulgazione interna di segnalazioni	PLC-100

Id	Ambito	Descrizione sintetica	Nome della procedura	Policy
Proc-03	Gestione degli incidenti	Procedura che consente di definire il flusso di lavoro per la rilevazione, l'identificazione e la classificazione degli eventi di sicurezza informatica proveniente dai canali interni dell'Amministrazione della Giustizia.	Procedura di rilevazione, identificazione e classificazione degli eventi interni	PLC-100
Proc-04	Gestione Software	Procedura per la catalogazione del software autorizzato e necessario a ciascun tipo di sistema (PdL, workstation, server) e apparato fisico connesso alla rete degli Uffici e delle Sale Server dell'Amministrazione della Giustizia.	Procedura di censimento del software	PLC-002
Proc-05	Gestione Hardware e Infrastruttura di rete	Procedura per la catalogazione e prioritizzazione delle reti, dei sistemi (PdL, workstation, server) e degli apparati fisici connessi alla rete di un Ufficio o Sala Server dell'Amministrazione della Giustizia.	Procedura di censimento delle reti, dei sistemi e degli apparati fisici	PLC-001, PLC-011,
Proc-06	Gestione Software	Procedura per l'autorizzazione all'installazione di software non compreso nell'inventario ufficiale dell'Ufficio o Sala Server, con l'iscrizione presso un apposito registro.	Procedura per l'installazione di software non inventariato.	PLC-002
Proc-07	Gestione dati	Procedura di censimento, classificazione e cifratura di tutti i flussi di dati e le comunicazioni/notificazioni in ingresso, in uscita, e interni ad un Ufficio Centrale, Ufficio Giudiziario o Sala Server.	Procedura di censimento, classificazione e cifratura dei flussi di dati	PLC-006, PLC-007

Id	Ambito	Descrizione sintetica	Nome della procedura	Policy
Proc-08	Gestione utenze	Procedura per la gestione delle utenze di amministrazione di PdL, workstation, server, dispositivi hardware e di rete, software e applicativi, per un Ufficio o Sala Server.	Procedura di gestione delle utenze di amministrazione.	PLC-017, PLC-018
Proc-09	Gestione utenze	Procedura per la gestione dell'inventario delle utenze di amministrazione di PdL, workstation, server, dispositivi hardware e di rete, software e applicativi, per un Ufficio o Sala Server.	Procedura di gestione dell'inventario delle utenze di amministrazione	PLC-019
Proc-10	Gestione utenze	Procedura per la gestione delle credenziali d'accesso degli utenti di amministrazione di una Sala Server o di un Ufficio Giudiziario	Procedura di gestione delle credenziali d'accesso delle utenze di amministrazione.	PLC-019, PLC-020, PLC-024
Proc-11	Gestione utenze	Procedura per la gestione delle utenze per PdL, software e applicativi, di un Ufficio o Sala Server	Procedura di gestione delle utenze non di amministrazione.	PLC-020, PLC-024
Proc-12	Gestione utenze	Procedura per la gestione delle credenziali d'accesso degli utenti non di amministrazione di una Sala Server o di un Ufficio Giudiziario	Procedura di gestione delle credenziali d'accesso delle utenze non di amministrazione.	PLC-020, PLC-024
Proc-13	Gestione chiave privata	Procedura per la gestione sicura delle chiavi private utilizzate all'interno di un Ufficio o Sala Server per operazioni di identificazione, autenticazione, autorizzazione, firma digitale e cifratura.	Procedura di gestione della chiave privata	PLC-025
Proc-14	Gestione dati	Procedura per la gestione dei back-up per il completo ripristino del sistema e dei dati su di esso memorizzati.	Procedura di gestione dei back-up dei server.	PLC-097

Id	Ambito	Descrizione sintetica	Nome della procedura	Policy
Proc-15	Gestione software	Procedura per la verifica e l'approvazione della documentazione tecnica accompagnante il rilascio di un software sviluppato da terze parti.	Procedura di gestione della documentazione tecnica dei software.	PLC-062, PLC-063
Proc-16	Gestione software	Procedura per il rilascio di patch e aggiornamenti di prodotti e di software applicativi per gli Uffici e le Sale Server, con la verifica sugli ambienti di test e pre-produzione, prima di essere installate nei sistemi in esercizio.	Procedura di rilascio patch e aggiornamenti.	PLC-053, PLC-054
Proc-17	Gestione vulnerabilità	Procedura che disciplina le modalità e la frequenza dell'attività di ricerca delle vulnerabilità presso un Ufficio o una Sala Server.	Procedura di gestione della ricerca delle vulnerabilità	PLC-082, PLC-118
Proc-18	Gestione della Rete	Procedura che disciplina l'autorizzazione e le modalità di segregazione della rete interna a un Ufficio o Sala Server, nonché le modalità di segmentazione della stessa (es. VLAN/subnetting, DMZ, VPN, ecc.).	Procedura di gestione della segregazione e della segmentazione.	PLC-032, PLC-033, PLC-035
Proc-19	Gestione sicurezza perimetrale	Procedura che disciplina le modalità di richiesta e di autorizzazione, per un Ufficio o una Sala Server al Centro Firewall di Napoli, dell'apertura o della chiusura di specifiche porte di rete verso l'esterno.	Procedura di richiesta e autorizzazione della gestione delle politiche di accesso gestite da firewall.	PLC-058

Id	Ambito	Descrizione sintetica	Nome della procedura	Policy
Proc-20	Gestione Digital Workspace	Procedura che disciplina la gestione delle PdL, avendo particolare riguardo alla: installazione e configurazione iniziale; installazione e aggiornamento del software di sistema; installazione e aggiornamento del software applicativo; limitazione alla connessione di supporti esterni o reti dati diverse da quelle appartenenti al perimetro di sicurezza e limitazioni alla modifica delle impostazioni da parte degli utenti.	Procedura di gestione del Digital Workspace	Da PLC-043 a PLC-056

12 (ALLEGATO A) NORMATIVA DI RIFERIMENTO

Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio, entrato in vigore il 25 Maggio 2016, operativo nei Paesi UE a decorrere dal 25 maggio 2018, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", pubblicato in Gazzetta Ufficiale Europea il 04/05/2016, come integrato dal D. lgs del 10 agosto 2018 n. 101;

Legge 7 agosto 1990, n. 241 e s.m.i. "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";

Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. "Codice dell'amministrazione digitale (CAD)";

Decreto Legislativo del 18 maggio 2018 n. 51 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati;

Decreto Legislativo 18 maggio 2018, n. 65, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";

D.P.R. 28 dicembre 2000, n. 445 e s.m.i. "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";

D.P.C.M. 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»";

D.P.C.M. 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";

D.P.C.M. 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";

D.P.C.M. 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese";

D.P.C.M. 15 giugno 2015, n. 84 "Regolamento di riorganizzazione del Ministero della Giustizia e riduzione degli uffici dirigenziali e delle dotazioni organiche";

D.P.C.M. 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali";

D.P.C.M. del 31 marzo 2017 di adozione del Piano Nazionale per la protezione cybernetica e la sicurezza informatica;

D.M. 27 marzo 2000, n. 264 "Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari";

D.M. 24 maggio 2001 ("Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia");

D.M. 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche

temporale, della posta elettronica certificata", pubblicato sulla Gazzetta Ufficiale n.266 del 15-11-2005;

D.M. 23 dicembre 2006 e s.m. ("Regolamento recante la disciplina del trattamento dei dati sensibili e giudiziari da parte del Ministero della giustizia");

D.M. 17 luglio 2008, "Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile", in sostituzione del decreto del Ministro della giustizia 14 ottobre 2004, pubblicato nel supplemento ordinario n.167 alla Gazzetta Ufficiale n.272 del 19 novembre 2004 – s.o. n. 184 alla Gazzetta Ufficiale n.180 del 2 agosto 2008;

D.M. 27 aprile 2009, "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia", pubblicato in Gazzetta Ufficiale n.107 del 11 maggio 2009;

D.M. 19 gennaio 2016 "Recante misure necessarie al coordinamento informativo ed operativo tra la Direzione generale per i sistemi informativi automatizzati del Dipartimento dell'Organizzazione giudiziaria, del personale e dei servizi e altre articolazioni del Ministero della giustizia, nonché concernente l'individuazione degli uffici di livello dirigenziale non generale e la definizione dei relativi compiti ai sensi dell'art.16 c1 e c2 del D.P.C.M. 84/2015" pubblicato nel B.U. del Ministero il 28 febbraio 2016;

"Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica" del Garante Privacy del 18 luglio 2013, pubblicato sulla Gazzetta Ufficiale n.189 del 13 agosto 2013;

Circolare AgID n. 3 del 6 dicembre 2016 "Regole Tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra sistemi telematici di acquisto e di negoziazione";

Circolare AgID del 18 aprile 2017 n. 2/2017 recante: "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";

Linee Guida per il disaster recovery delle pubbliche amministrazioni emanate dall'AgID ai sensi del c. 3, lettera b) dell'art. 50 bis del Codice dell'Amministrazione Digitale (aggiornamento 2013);

Determinazione AgID n.219/2017, Approvazione e pubblicazione delle "Linee guida per transitare al nuovo modello di interoperabilità";

Decreto ministeriale 23 aprile 2020. Misure necessarie al coordinamento informativo ed operativo tra la Direzione generale per i sistemi informativi automatizzati del Dipartimento dell'Organizzazione giudiziaria, del personale e dei servizi e altre articolazioni del Ministero della giustizia, nonché individuazione degli uffici di livello dirigenziale non generale e definizione dei relativi compiti ai sensi dell'articolo 16, commi 1 e 2, del decreto del Presidente del Consiglio dei ministri 15 giugno 2015, n. 84 e dell'articolo 6, comma 2, del decreto del Presidente del Consiglio dei ministri 19 giugno 2019, n. 99.

13 (ALLEGATO B) CONTROLLI DI SICUREZZA

Altamente riservato (L5).