Ministero dell'Economia e delle Finanze
Dipartimento delle Finanze

Area Organizzativa Omogenea

Ufficio di Segreteria del

Consiglio di Presidenza della Giustizia Tributaria

MANUALE DI GESTIONE DOCUMENTALE
per la tenuta del protocollo informatico,
dei flussi documentali e degli archivi

Versione 1.0 del 16 marzo 2016

INTRODUZIONE

Il presente Manuale di gestione documentale, previsto dall'articolo 5 del D.P.C.M. 3 dicembre 2013[1], "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

Viene adottato ai sensi dell'art. 3 delle *Regole tecniche protocollo* dal coordinatore della gestione documentale designato nel Dipartimento delle finanze su proposta del responsabile della gestione documentale dell' Area Organizzativa Omogenea in intestazione.

Infatti, è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee (*AOO)*[2] - all'interno delle quali sia nominato un responsabile della gestione documentale, e un suo vicario per i casi di vacanza, assenza o impedimento del primo nonché, nell'ambito delle amministrazioni con più aree organizzative omogenee, il coordinatore della gestione documentale e un suo vicario[3].

Per l'individuazione delle *AOO*, dei relativi responsabili della gestione documentale e del coordinatore nell'ambito del Dipartimento delle finanze si rimanda agli allegati 2 e 3.

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso, in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti interni ed esterni che a diverso titolo interagiscono con l'amministrazione.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l' Area Organizzativa Omogenea interessata ed è reso pubblico mediante pubblicazione: sul sito internet istituzionale del Dipartimento delle finanze (www.finanze.gov.it) e sul sito intranet dipartimentale (https://intranet.mef.gov.it).

---

[1] 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" (di seguito "*Regole tecniche protocollo*")

[2] Vedi art. 50, comma 4, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000), di seguito indicato con "T*esto unico*"

[3] Vedi art. 61, comma 2, del Testo unico e art. 3, comma 1 delle *Regole tecniche protocollo*

SEZIONE 1 – DISPOSIZIONI GENERALI E DEFINIZIONI

1. Ambito di applicazione del Manuale

Il presente Manuale di gestione è adottato ai sensi dell'art. 5 delle R*egole tecniche protocollo informatico*. Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi della AOO corrispondente all'Ufficio di Segreteria del Consiglio di Presidenza della Giustizia Tributaria e agli Uffici in cui è suddivisa (articolazioni di livello non dirigenziale definite nella Deliberazione del Consiglio di Presidenza della giustizia tributaria del 19.03.2002 che approva il Regolamento per l'organizzazione e il funzionamento di Segreteria e successive modifiche e integrazioni).

2. Riferimenti normativi

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

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428" (in vigore fino al 11.8.2016);

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (indicato nel Manuale con "*Testo unico*")

Decreto del Presidente della Repubblica 8 gennaio 2001, n. 37, "Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli *Uffici* dello Stato ;

Decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni "Codice in materia di protezione dei dati personali";

Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004 "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali" (in vigore fino al 11.4.2017);

Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'*Amministrazione* digitale" e successive modifiche e integrazioni (indicato di seguito nel Manuale con "*CAD"*);

Decreto legislativo 30 dicembre 2010 n. 235 - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005 n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69;

Decreto del Presidente del Consiglio dei ministri 22 febbraio 2013 «Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71», pubblicato nella Gazzetta Ufficiale 21 maggio 2013, n. 117;

Decreto del Presidente del Consiglio dei Ministri 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, pubblicato nella Gazzetta Ufficiale 12 marzo 2014, n. 59 (di seguito nel Manuale "*Regole tecniche conservazione*")

Decreto del Presidente del Consiglio dei Ministri 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, pubblicato nella Gazzetta Ufficiale 12 marzo 2014, n. 59 (di seguito nel Manuale "*Regole tecniche protocollo*")

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, pubblicato nella Gazzetta Ufficiale 12 gennaio 2015, n. 8 (di seguito nel Manuale "*Regole tecniche documento*")

3. Definizioni

Ai fini del presente Manuale s'intende:

- per ***Amministrazione*** [in *corsivo* nel Manuale], il Dipartimento delle Finanze (DF) del Ministero dell'economia e delle finanze (MEF);
- per ***Amministrazione finanziaria*** [in *corsivo* nel Manuale], il Dipartimento delle Finanze (DF) del Ministero dell'economia e delle finanze (MEF) e le Agenzie fiscali;
- per ***archivio corrente***, la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse corrente;
- per ***archivio storico***, il complesso di documenti relativi ad affari esauriti e destinati, previe operazioni di scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico;
- per ***area organizzativa omogenea*** (*AOO*) [in *corsivo* nel Manuale], un insieme di funzioni e di strutture, individuate dall'*Amministrazione*, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***assegnazione***, l'operazione d'individuazione dell'*Ufficio*/*Utente* competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;

- per ***classificazione***, attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- ***per Coordinatore della gestione documentale***, il responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le *AOO* ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche*);
- per ***Uffici*** [in *corsivo* nel Manuale], la Direzione dell'Ufficio di Segreteria del Consiglio di Presidenza della Giustizia Tributaria e le sue articolazioni previste dall'art. 6 del Regolamento per l'organizzazione e il funzionamento di Segreteria e successive modifiche e integrazioni (Deliberazione del Consiglio di presidenza della giustizia tributaria del 19 marzo 2002) ;
- per ***documento amministrativo***, ogni rappresentazione grafica, fotocinematografica, informatica o di qualsiasi altra specie del contenuto di atti, fatti o cose giuridicamente rilevanti, anche interni, prodotti e acquisiti ai fini dell'attività amministrativa, così come prevede l'art. 22 comma 2 della legge 7 agosto 1990, n. 241. Un documento amministrativo è dunque una rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa, così come prevede l'art. 1 del *Testo unico*;
- per ***documento informatico***, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, ai sensi dell'art. 1, comma 1, lettera p) del Decreto Legislativo 7 marzo 2005, n. 82;
- per ***fascicolo informatico***, l'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche)*
- per ***fascicolazione***, l'operazione di riconduzione dei singoli documenti classificati in uno o più fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;
- per ***firma digitale***, il risultato della procedura informatica basata su un certificato qualificato e su sistema di chiavi crittografiche asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (vedi art. 1 lett. s) del *CAD)*;
- per ***formato***, la modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***Ente*** [in *corsivo* nel Manuale], la struttura organizzativa dell'Amministrazione finanziaria (Dipartimento delle finanze o Agenzia fiscale)

- per ***impronta di un documento informatico***, "una sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash" (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche)* in grado di identificarne univocamente il contenuto;
- per ***manuale di conservazione***, *lo* strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***manuale di gestione*** [ovvero nel seguito: Manuale]**,** *lo* strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle *Regole tecniche protocollo* (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***piano di conservazione degli archivi*****,** lo strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e conservazione dei documenti, ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***Posta Elettronica Certificata (PEC***) [in *corsivo* nel Manuale]**,** il sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici, mentre convenzionalmente con la sigla *PEL* (Posta Elettronica) [in *corsivo* nel Manuale] viene indicato il sistema di posta elettronica che non fornisce attestazioni di invio e di consegna con valenza legale;
- per ***regole tecniche*** [in *corsivo* nel Manuale], l'insieme delle norme attuative del Codice dell'Amministrazione Digitale e nello specifico del presente Manuale:
  Regole tecniche conservazione (DPCM 3.12.2013), *Regole tecniche protocollo* (DPCM 3.12.2013) *Regole tecniche documento* (DPCM 13.11.2014) [vedi paragrafo: Riferimenti normativi]
- per ***responsabile della conservazione*** [in *corsivo* nel Manuale]**,** il soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***responsabile della gestione documentale (RgD) (o responsabile del servizio di gestione documentale ovvero responsabile per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi***) [in *corsivo* nel Manuale]**,** il dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, che nella *AOO* del presente Manuale è preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione (vedi Glossario/Definizioni – Allegato 1 alle *Regole tecniche);*
- per ***Servizio di gestione documentale (SgD)*** [in *corsivo* nel Manuale]**,** l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, *assegnazione* e reperimento dei documenti amministrativi, informatici e analogici, formati o acquisiti dall'*Amministrazione*, nell'ambito del sistema di classificazione adottato (cfr. anche art. 1 lett u) del *CAD* per la gestione informatica dei documenti);

- per ***Servizi Documentali (SD)*** [in *corsivo* nel Manuale]**,** l'insieme degli applicativi integrati che assicurano la gestione documentale nelle strutture organizzative dell'*amministrazione finanziaria* (Dipartimento delle finanze e Agenzie fiscali);
- per ***segnatura di protocollo***, l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso, che consente di individuare il documento in modo inequivocabile (v. art. 55, comma 1, del *Testo unico*;
- per ***supporto di memorizzazione***, il mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso;
- per ***Testo unico*** [in *corsivo* nel Manuale]**,** il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, pubblicato con DPR 28 dicembre 2000, n. 445;
- per ***Titolario di classificazione*** [in *corsivo* nel Manuale], un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'*Amministrazione*, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta;
- per ***Utenti*** [in *corsivo* nel Manuale], le persone dell'*Amministrazione* che utilizzano i servizi messi a disposizione dal sistema di gestione informatica dei documenti.

4. Aree Organizzative Omogenee (*AOO*) e responsabili

Ai fini della gestione dei documenti, l'*Amministrazione* ha individuato le *Aree Organizzative Omogenee* centrali e periferiche con Decreto del Direttore Generale delle Finanze del 5/11/2015 (Allegato 2) e designato i relativi *Responsabili della gestione documentale* (RgD), e con Decreto del Direttore Generale delle Finanze del 5/11/2015 (Allegato 3) il *Coordinatore della gestione documentale* dell'*Ente* Dipartimento delle Finanze.
Il presente Manuale si applica alla gestione documentale della *AOO* di cui al paragrafo 1, le cui schede descrittive sono riportate nell'allegato 1.

5. Servizio per la gestione documentale (*SgD*)

Nell'ambito della *AOO* del presente Manuale è istituito il "Servizio per la gestione documentale" (*SgD*).

Esso è funzionalmente costituito all'interno dell'*Ufficio* di Segreteria del Consiglio di Presidenza della Giustizia Tributaria e fa capo al dirigente incaricato, nonché Responsabile della gestione documentale (RgD), ed in ultima istanza, al direttore della *Direzione*/*Dipartimento*.

I compiti dei Responsabili della gestione documentale sono previsti dall'art. 4 delle *Regole tecniche protocollo* e dall'art. 61 del *Testo unico*.

Nei casi di vacanza, assenza o impedimento del Responsabile, la direzione del Servizio è affidata al vicario nominato su proposta del Responsabile stesso (art. 3, lettera *b*, delle R*egole tecniche protocollo)*.
Il Responsabile *SgD* individua una o più persone, idonee a svolgere il ruolo di "Amministratore di *AOO*" i cui compiti riguardano la gestione operativa degli applicativi dedicati alla gestione documentale in relazione a abilitazioni all'accesso degli utenti, assegnazione di ruoli e permessi, gestione dei registri, gestione dei piani di classificazione e fascicolazione, etc.

Al Servizio sono assegnati i seguenti compiti (art. 61, comma 3, del *testo unico)* assolti attraverso le funzionalità dell'applicativo informatico Protocollo (vedi par. 9):

a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del *Testo unico*;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'art. 53;
d) cura che le funzionalità del sistema, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le informazioni del sistema (art. 62) e il Registro di emergenza (art. 63) in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
g) autorizza le operazioni di annullamento di cui all'art. 54;
h) vigila sull'osservanza delle disposizioni del *Testo unico* da parte del personale autorizzato e degli incaricati.

In considerazione di quanto previsto dall'art. 3, comma 1, lett. c) delle *Regole tecniche protocollo*, cioè la nomina, nell'ambito delle amministrazioni con più *AOO*, del coordinatore della gestione documentale e del suo vicario, il Dipartimento delle finanze ha designato tali figure (vedi Allegato 3), il cui ambito di competenza è riferito ai documenti amministrativi prodotti dalle strutture centrali, dalle Commissioni tributarie del Dipartimento delle Finanze e dall'Ufficio di Segreteria del Consiglio di Presidenza della giustizia tributaria; in particolare il coordinatore, ai sensi dell'art. 4, comma 2 delle citate *Regole tecniche*, ha il compito di interagire con i Servizi di gestione documentale delle *AOO* e con i rispettivi Responsabili, al fine di definire e assicurare criteri uniformi di trattamento dei documenti e, in particolare, di classificazione e archiviazione, nonché di comunicazione interna tra le *AOO* del Dipartimento delle finanze.

6. Servizi Documentali

Nella *AOO* del presente *Manuale,* la gestione documentale è realizzata mediante il sistema "*Servizi Documentali"*, insieme di vari applicativi informatici integrati tra loro, utilizzati da tutte le *AOO* degli *Ent*i dell'*Amministrazione finanziaria*. Tra gli applicativi in uso presso le suddette *AOO*:

- Protocollo, componente che garantisce la tenuta del protocollo informatico ai sensi dell'art.61, comma 1 del *testo unico* [di seguito nel Manuale in grassetto: **Protocollo**]

- Amministrazione(**SGSU,** Sistema di Gestione della Sicurezza Unificato), componente attraverso cui si definiscono e vengono gestiti gli Uffici e gli utenti della *AOO*, i permessi applicativi e l'assegnazione dei ruoli agli utenti relativamente ai servizi documentali [di seguito nel Manuale in grassetto: **Amministrazione**]

- Fascicoli, componente che consente l'aggregazione dei documenti in fascicoli e la loro gestione [di seguito nel Manuale in grassetto: **Fascicoli**]

- Titolario, componente che consente la gestione nel tempo di un *titolario di classificazione* unico per *Ente*, definito per tutti i tipi documento prodotti nell'ambito dell'Ente e che possa essere richiamato dalle varie applicazioni. Lo stesso *titolario* è realizzato nell'ottica della futura gestione della fascicolazione automatica dei documenti e delle procedure di scarto d'archivio e conservazione [di seguito nel Manuale in grassetto: **Titolario**]

- Firma, ovvero l'applicazione che consente ai titolari di firma digitale di firmare i documenti di propria competenza. L'apposizione della firma può essere effettuata sul singolo documento o in modo massivo su più documenti [di seguito nel Manuale in grassetto: **Firma**]

7. Ruoli organizzativi e ruoli applicativi

I ruoli organizzativi, definiti in coerenza con le responsabilità all'interno dell'organizzazione, sono ruoli trasversali a tutti gli applicativi dei Servizi Documentali. Tali ruoli vengono assegnati e gestiti sull'applicativo **Amministrazione (SGSU)**. Nel dettaglio, sono:

- Il Responsabile (Dirigente o altro funzionario responsabile incaricato presso ciascun *Ufficio*) ha l'accesso a tutti i documenti e i fascicoli del proprio *Ufficio*; riceve tutti i documenti in ingresso assegnati per competenza al proprio *Ufficio* e li assegna per la trattazione ai dipendenti; è responsabile della corretta ed esaustiva classificazione e fascicolazione dei documenti trattati dall'*Ufficio*; è responsabile dei documenti prodotti in uscita dal proprio *Ufficio*, curandone la sottoscrizione da parte del Direttore;
- Il Facente Funzione: il Responsabile individua tra le persone a lui assegnate il proprio Facente Funzione al quale demanda le proprie funzioni in caso di assenza, impedimento, o per specifico incarico;
- L'Assegnatario per l'Ufficio: è colui che è abilitato a ricevere e gestire i documenti e le attività assegnati all'ufficio . In ogni ufficio deve essere definito almeno un assegnatario.
- La Segreteria: ha la possibilità di visualizzare le attività in carico al proprio Ufficio e agli Uffici ad esso gerarchicamente subordinati, e può visualizzare i protocolli registrati nel proprio ufficio e negli uffici ad esso gerarchicamente subordinati.

I ruoli organizzativi devono essere completati dai ruoli specifici nell'applicativo di riferimento.

****

I ruoli applicativi sono i ruoli tipici di uno specifico applicativo. Attraverso questi ultimi vengono regolati accesso e funzionamento dei singoli applicativi nonché l'insieme di funzionalità del sistema accessibili al singolo utente.
Alcuni Ruoli applicativi di base e le relative autorizzazioni vengono gestiti su **Amministrazione**.
Per l'applicativo Protocollo sono gestititi su SGSU i seguenti ruoli applicativi:

- ◊ Protocollatore: il ruolo di "Protocollatore" aggrega i permessi di protocollazione in ingresso, in uscita e registrazione. Inoltre consente di protocollare anche i documenti classificandoli con dati sensibili. Il ruolo di Protocollatore ha validità all'interno del singolo Ufficio;
- ◊ Protocollatore Riservato: questo ruolo consente di visualizzare i documenti riservati nel rispetto delle vigenti regole di visibilità e, la protocollazione di documenti riservati, a condizione che, nell'ufficio, l'attore abbia anche il ruolo di "Protocollatore";
- ◊ Gestore dati sensibili: il ruolo di "Gestore dati sensibili" è applicato a livello di *AOO* e consente la visualizzazione dei documenti con dati sensibili, senza necessità di richiedere l'autorizzazione a tempo sul singolo protocollo, nel rispetto delle vigenti regole di visibilità.

L'applicativo **Protocollo**, nella sua configurazione standard, dispone inoltre di ulteriori ruoli predefiniti e validi solo all'interno dell'applicativo stesso, tra i quali:

- ◊ Amministratore di Ente: creazione e gestione delle Aree Organizzative Omogenee, *Uffici*, Ruoli, Utenti; funzionalità di gestione delle estensioni e di amministrazione dell'applicativo;
- ◊ Amministratore di *AOO*: gestione dell'Area Organizzativa Omogenea di propria competenza, degli Utenti, degli *Uffici*, dei Permessi, dei Registri, del Piano di classificazione e delle funzionalità di gestione delle estensioni;
- ◊ Operatore/Utente: l'Operatore/utente ha accesso a tutti i fascicoli dell'Ufficio di appartenenza e ai documenti ad esso assegnati direttamente. Ha funzionalità di Protocollazione e accesso ai Registri di protocollo. E' incaricato della trattazione dei documenti e provvede alla corretta classificazione e fascicolazione degli stessi.

Infine, su **Protocollo** è possibile creare ulteriori ruoli tramite l'attivazione dei permessi associati alle funzionalità applicative. In tal modo è possibile ad esempio sviluppare ruoli, validi all'interno dell'applicativo stesso, in grado di soddisfare obiettivi specifici o determinate esigenze organizzative.

Il Responsabile del *SgD* assegna ad ogni utente dell'*AOO* uno o più ruoli applicativi, in coerenza con la posizione organizzativa e le funzioni assegnate a ciascuno, e secondo le necessità *dell'Ufficio di Segreteria*. E' possibile assegnare alla stessa persona due o più ruoli applicativi.

SEZIONE 2 - FORMAZIONE DEI DOCUMENTI

8. Modalità di formazione dei documenti e contenuti minimi

I documenti di ciascuna *AOO* sono prodotti dagli *Utenti* con sistemi informatici, ai sensi dell'articolo 9 delle *Regole tecniche documento* e dell'art. 40 del *CAD*.
Le regole per la determinazione dei contenuti e della struttura dei documenti sono definite dalla dirigenza ai sensi dell'art. 4, comma 2, del D.lgs.165/2001. Su di essi devono essere obbligatoriamente riportate le seguenti informazioni:

- denominazione e stemma dell'*Amministrazione*;
- indicazione completa dell'*Ufficio* che ha prodotto il documento, con indirizzo completo, numero di telefono, indirizzo di posta elettronica;
- data completa e n° di registrazione desumibili dalla segnatura di protocollo
- numero degli allegati, se presenti;
- oggetto del documento;
- denominazione completa del destinatario, con indirizzo elettronico (per documenti in uscita dalla *AOO*)
- sottoscrizione del Responsabile, o dei Responsabili, quando prescritta.

N.B.
Ai sensi di quanto previsto dalle *Regole tecniche documento*, l'Amministrazione, a partire dall'11 Agosto 2016, deve produrre gli originali dei propri documenti esclusivamente in formato digitale.

9. Formato dei documenti amministrativi informatici

Ai fini della formazione e della gestione del documento amministrativo informatico sul sistema documentale, come previsto dalle *Regole tecniche protocollo* e dalle *Regole tecniche documento*, si riportano di seguito i formati ammessi:

Acrobat PDF
BMP Image (BitMap)
Firmati digitalmente in modalità CADES
GIF Image
JPEG Image
Microsoft Office Excel
Microsoft Office Word
Open Office Document (odt)
Portable Network Graphics (PNG)
TIFF Image
XML

Il documento amministrativo informatico, indipendentemente dal software utilizzato, prima della sottoscrizione con *firma digitale*, è prodotto con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo

del contenuto e della struttura. Si adotta preferibilmente il formato PDF. I documenti informatici redatti dall'*AOO* con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con *firma digitale*, nei formati standard PDF come previsto dalle *Regole tecniche conservazione* (DPCM 3 dicembre 2013), al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

10. Sottoscrizione dei documenti: firma digitale e firma autografa

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta di norma con un processo di *firma digitale* conforme alle disposizioni dettate dalla normativa vigente (Codice di Amministrazione digitale, artt. 24-37).
L'*Amministrazione* si avvale a tale scopo dei servizi di una Certification Authority iscritta nell'elenco pubblico dei certificatori tenuto dall'AgID.
Tra i servizi documentali a disposizione dell'Amministrazione vi è l' applicazione di Firma Digitale che consente ai titolari del certificato di firmare i documenti di propria competenza. L'apposizione della firma può essere effettuata su di un singolo documento o in modo massivo su più documenti contemporaneamente. Durante l'operazione di firma, il firmatario potrà utilizzare la smart card, un token in suo possesso oppure potrà utilizzare il certificato memorizzato su un dispositivo remoto Hardware Security Module (HSM), ovvero la soluzione di firma elettronica centralizzata.
Nel sistema sono previste funzioni automatiche di verifica della *firma digitale* sui documenti e sugli eventuali allegati da fascicolare.

N.B.
La sottoscrizione dei documenti con firma autografa, previa stampa del documento informatico, è consentita esclusivamente nei casi di impedimento accertato nell'apposizione della *firma digitale* o nella spedizione del documento su supporto informatico.

SEZIONE 3 - MODALITÀ DI RICEZIONE/TRASMISSIONE DEI DOCUMENTI

11. Flusso organizzativo dei documenti in ingresso

- Il Servizio di gestione documentale (*SgD)* riceve i documenti in ingresso
- Il *SgD* provvede alla registrazione e segnatura di protocollo, alla classificazione ed eventualmente alla codificazione per il Controllo di gestione;
- Il *SgD* assegna i documenti all'*Ufficio* (e/o all'*Utente)* per competenza di trattazione ed eventualmente ad altri *Uffici* per conoscenza
- Il Responsabile (Funzionario preposto o suo incaricato) dell'*Ufficio* assegnatario assegna per la trattazione al dipendente (*Utente*)
- L'*Utente* assegnatario, secondo le indicazioni del Responsabile della gestione documentale, effettua la fascicolazione del documento assegnato

12. Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono pervenire alla *AOO* attraverso:

a) il servizio postale tradizionale o interno;
b) la consegna diretta al *SgD*;
c) gli apparecchi telefax.

I documenti che transitano attraverso il servizio postale tradizionale sono ritirati ogni giorno a cura del personale addetto al servizio automobilistico o in caso di assenza o impedimento da personale incaricato dal *RgD* .
Tutti i documenti su supporto cartaceo pervenuti alla *AOO* vengono consegnati al *SgD*.
I documenti soggetti a registrazione di protocollo (vedi Sezione 4 – Registrazione dei documenti), consegnati direttamente agli *Utenti* non abilitati alla loro protocollazione, sono fatti pervenire al *SgD*, a cura del personale che li riceve e nell'arco della stessa giornata.
I documenti ricevuti con apparecchi telefax, se soggetti a registrazione di protocollo, sono trattati come quelli consegnati direttamente agli *Utenti*.
Nella successiva Sezione 4 - Registrazione dei documenti - sono trattate le modalità di registrazione per i documenti che costituiscono eccezioni a quanto suddetto.

Sui documenti ricevuti su supporto cartaceo il *SgD* effettua, ovvero cura che siano effettuate, le seguenti operazioni:

- ricezione: apertura buste, autenticazione (esame al fine di verificarne la provenienza)
- registrazione di protocollo
- scansione dei documenti per l'acquisizione in formato elettronico
- segnatura di protocollo sul documento cartaceo
- assegnazione all'*Ufficio* (o se del caso direttamente all'*Utente)* competente per la trattazione
- consegna dell'originale cartaceo all'*Ufficio* assegnatario.

Per quanto riguarda procedure e regole per la scansione dei documenti si veda il paragrafo 29.

N.B.
Le modalità di ricezione dei documenti cartacei illustrate nel presente paragrafo sono destinate a diventare residuali, e comunque esclusivamente ammesse per la ricezione di documenti inviati da mittenti pubblici e privati non soggetti alle prescrizioni del *CAD* e delle *Regole tecniche* (ad es. cittadini privati sprovvisti di identità e indirizzo digitale), mentre tutte le pubbliche amministrazioni soggette al *CAD* entro l'11 agosto 2016 devono adeguarsi allo scambio esclusivo di documenti informatici.

13. Ricezione dei documenti informatici

La ricezione dei documenti informatici è assicurata tramite:

- **casella di posta elettronica certificata (*PEC*) e casella di posta elettronica (PEL)** integrate, direttamente associate al registro di protocollo, riservate a questa funzione ed accessibili solo al *SgD* tramite i ruoli applicativi del sistema di protocollo.
  Gli indirizzi di tali caselle sono:

  ufficiosegreteriaCPGT@pce.finanze.it

  pubblicato sull'indice delle P.A. all'indirizzo http://www.indicepa.gov.it

  e

  nsd.cpgt.protocollo@finanze.it

  pubblicato sul sito www.giustizia-tributaria.it

- **comunicazione tra *AOO* dell'Amministrazione finanziaria**

  (nuova funzionalità rilasciata il 1/12/2015)

  Le comunicazioni tra *AOO* dello stesso *Ente* o di altri Enti dell'*Amministrazione finanziaria* avvengono mediante la funzione dedicata che consente lo scambio di documenti tra *AOO* senza utilizzare l'infrastruttura di *PEC* e le relative le caselle *PEC* integrate nel sistema, rendendo quindi più snello il processo di creazione dei messaggi di posta, di scarico dei messaggi dalle caselle ed elaborazione degli stessi, poichè sfrutta l'infrastruttura del repository comune dei dati tra *AOO* dell'*Amministrazione Finanziaria*.
  Pertanto, al fine di alleggerire il sistema di trasmissione tramite *PEC* ed uniformare le modalità di trasmissione/ricezione, le *AOO* del Dipartimento delle finanze usano esclusivamente tale canale di comunicazione per scambiare documenti tra di loro e con le *AOO* delle Agenzie fiscali, riservando l'uso della *PEC* solo nell'ipotesi di necessità della ricevuta di avvenuta consegna

14. Rilascio di ricevute attestanti la ricezione dei documenti

Qualora venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna di un documento cartaceo ovvero pervenuto tramite caselle funzionali non integrate nel sistema di Protocollo, il *SgD* rilascia la relativa ricevuta nelle modalità previste.

Nel caso di ricezione dei documenti informatici tramite casella *PEC*, si fa riferimento a quanto descritto nel paragrafo 18.

15. Flusso organizzativo dei documenti in uscita

- I documenti sono formati dagli *Utenti* della *AOO*
- Gli *Utenti* provvedono ad acquisire l'assenso del Responsabile del competente *Ufficio* della *Direzione* sul documento formato e lo rendono disponibile per la firma
- Il Responsabile dell'*Ufficio* (funzionario o suo incaricato) provvede a firmare il documento ovvero a farlo firmare digitalmente o autografare dal Direttore dell'Ufficio di Segreteria del Consiglio di Presidenza della Giustizia Tributaria ovvero dal Presidente del Consiglio di Presidenza della Giustizia tributaria o dal Consigliere Delegato.
- Il *SgD* provvede alla registrazione in uscita e alla spedizione
- Il SgD assegna il documento all'*Ufficio*/*Utente*, effettua la classificazione e la codificazione per il Controllo di gestione;
- L'*Utente* assegnatario, secondo le indicazioni del Responsabile della gestione documentale, effettua la fascicolazione, del documento assegnato

16. Invio dei documenti informatici

L'invio dei documenti informatici è assicurata tramite:

- **casella di posta elettronica certificata (*PEC*) e casella di posta elettronica (PEL)**

  Per l'invio dei documenti informatici a destinatari esterni all'*Amministrazione finanziaria*, l'*AOO* si avvale del servizio di *PEC e PEL*, cioè tramite la casella *PEC* della AOO integrata nell'applicativo Protocollo (vedi paragrafo 13), in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche a determinati utenti (responsabile, facente funzione e assegnatari degli uffici in cui è stata effettuata la protocollazione), descritte nel paragrafo 18 e tramite la casella PEL della AOO integrata nell'applicativo Protocollo (vedi paragrafo 13) per inoltrare i messaggi a soggetti non in possesso di casella PEC;

- **comunicazione tra *AOO* dell'Amministrazione finanziaria**

  Per l'invio dei documenti informatici a destinatari interni all'Amministrazione finanziaria, l'*AOO* adotta la funzionalità "comunicazione tra *AOO* dell'Amministrazione finanziaria", come descritto al par. 13

17. Spedizione dei documenti su supporto cartaceo

La spedizione di documenti cartacei avviene esclusivamente nelle ipotesi di accertata impossibilità di trasmissione telematica dei documenti.

Gli *Utenti* devono far pervenire i documenti in partenza al *SgD* compresi i documenti riservati.
Nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere o altro mezzo che richieda una qualche documentazione da allegare alla busta, questa modulistica viene compilata dagli addetti al *SgD*.
I documenti da spedire su supporto cartaceo sono consegnati al *SgD* il quale effettua la registrazione di protocollo e segnatura e assegna per competenza all'*Ufficio* (o all'*Utente)*, che ha chiesto la spedizione.
Il *SgD* provvede direttamente alla trasmissione "fisica" del documento cartaceo in partenza e alla spedizione, di norma il giorno successivo lavorativo a quello in cui è stato protocollato.

N.B.
Le modalità di spedizione dei documenti cartacei illustrate nel presente paragrafo sono destinate a diventare residuali, e comunque esclusivamente ammesse per la spedizione di documenti verso privati non soggetti alle prescrizioni del *CAD* e delle *Regole tecniche* (ad es. cittadini privati sprovvisti di identità e indirizzo digitale), mentre tutte le pubbliche amministrazioni soggette al *CAD* entro l'11 agosto 2016 devono adeguarsi allo scambio esclusivo di documenti informatici.

18. Servizio di Posta Elettronica Certificata (*PEC*)

Il servizio è fornito da Sogei, certificatore iscritto nell'elenco pubblico tenuto dall'AgID, così come disposto dalla Direttiva europea 1999/93/CE, dal Regolamento eIDAS 910/2014/EC, dal DPCM 22 febbraio 2013 e dal *CAD*.

- **CARATTERISTICHE E LIMITI**

La casella di *PEC* della *AOO*

ufficiosegreteriaCPGT@pce.finanze.it

integrata e direttamente associata al registro di protocollo della *AOO medesima*, può correttamente colloquiare ***esclusivamente*** con altre caselle di *PEC;* quindi, non accettano posta proveniente da caselle NON-PEC, mentre l'invio verso utenti *NON-PEC* è possibile, ma subordinato al supporto del sistema di posta destinatario (*NON-PEC*) di protocolli sicuri quali SMTP -Simple Mail Transfer Protocol- su TLS -Transport Layer Security.

Nello specifico le casella *PEC* della *AOO* sopra citata può essere utilizzata per inviare posta verso tutte le caselle di posta elettronica non certificata (*PEL*) dell'Amministrazione Finanziaria.

Nel comporre il messaggio di *PEC*, sia il mittente esterno alla *AOO* che vuole inviare un messaggio alla *AOO*, sia l'operatore della *AOO* che vuole inviare in uscita un messaggio, devono fare attenzione ad alcuni aspetti, che potrebbero creare problemi sia nella ricezione del messaggio in ingresso, sia nell'invio del messaggio in uscita.

Di seguito alcuni accorgimenti da tener presenti:

1. non allegare al messaggio *PEC* un messaggio di posta in quanto il sistema di protocollo del destinatario potrebbe non essere in grado di individuare correttamente gli allegati e quindi di acquisire correttamente i documenti e gli allegati in ingresso;

2. la dimensione massima di tutto il messaggio (documento principale e allegati) è di 25 MB (MegaByte);

3. non tutti i caratteri speciali sono ammessi nel nome dei file del documento principale e degli allegati (è importante ricordare che l'utilizzo di caratteri speciali non è consentito neppure per i nomi dei file che vengono compressi nei formati .zip e .rar); gli unici caratteri ammessi sono:

   - i numeri
   - le lettere dell'alfabeto (minuscole e maiuscole)
   - l'underscore, il trattino e il punto;

4. non tutte le estensioni degli allegati sono ammesse. L'estensione di un file è un suffisso, ovvero una breve sequenza di caratteri alfanumerici (tipicamente tre o quattro), posto alla fine del nome di un file e separato dalla parte precedente con un punto, attraverso il quale è possibile distinguere il tipo di contenuto (testo, immagine...) e il formato utilizzato.
   Le estensioni ammesse sia per il documento principale sia per gli allegati della *PEC* sono riportate nel paragrafo 9.

- **RICEVUTE**

L'utilizzo della posta elettronica certificata (*PEC*) consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di *PEC* dell'*AOO* ricevente.

Questi ultimi sono:

- ✓ Ricevuta di accettazione, emesso del sistema di *PEC* del mittente che ha accettato il messaggio;
- ✓ Ricevuta di consegna, emessa dal sistema di *PEC* mittente a valle della consegna del messaggio da parte del sistema di *PEC* del destinatario, la ricevuta viene generata quindi solo nel caso in cui il messaggio sia stato inviato ad una casella di *PEC*;
- ✓ Avviso di mancata accettazione, emesso del sistema di *PEC* del mittente;
- ✓ Avviso di mancata consegna, nel caso in cui il sistema di *PEC* del destinatario abbia inviato l'avviso di impossibilità di recapitare il messaggio alla casella di *PEC* del destinatario;
- ✓ Avviso di mancata consegna per superamento tempo massimo, nel caso in cui il sistema di *PEC* del mittente non abbia ricevuto la ricevuta di avvenuta consegna da parte del sistema di *PEC* del destinatario trascorse le 24 ore dall'accettazione.

- **VALIDITA' LEGALE**

Ai sensi dell'art. 48 del *CAD* la trasmissione di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante posta elettronica certificata.
La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuto invio e l'avvenuta consegna, equivale alla notificazione per mezzo della posta.
La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso con *PEC* sono opponibili ai terzi.

Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore (art. 45 del *CAD)*.

SEZIONE 4 - REGISTRAZIONE DEI DOCUMENTI

19. Registrazione dei documenti

All'interno dell'*AOO* tutti i documenti rilevanti ai fini dell'attività amministrativa devono essere oggetto di registrazione. Tale registrazione è prevista dall'art. 53 del DPR 445/2000 ed ha la funzione giuridica di certificare la produzione dei documenti e garantire le operazioni di ricezione e di invio dei documenti da parte dell'*AOO*, consentendo inoltre di tenere traccia delle movimentazioni degli stessi.

20. Registro informatico di protocollo

Nell'ambito dell'*AOO,* tutte le operazioni di registrazione dei documenti sono effettuate esclusivamente tramite il sistema di Protocollo informatico. Non sono ammessi altri protocolli di settore e di reparto, e in generale protocolli diversi dal Protocollo informatico (art. 3 comma 1 lett. e) *Regole tecniche protocollo*).
A tal fine in ciascuna *AOO* viene istituito il Registro Ufficiale di protocollo che si apre il 1° gennaio e si chiude al 31 dicembre di ogni anno e contiene la numerazione unica e rigidamente progressiva delle registrazioni di protocollo dei documenti in entrata e in uscita dalla *AOO*.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il numero di protocollo è costituito da almeno sette cifre numeriche (art. 57 del *testo unico*).
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti hanno alcuni elementi comuni o sono strettamente correlati tra loro (art. 55 del *testo unico*).

N.B.
Per specifiche esigenze (modalità particolari di ricezione/invio, particolari categorie di documenti, etc.) possono essere istituti ulteriori Registri di corrispondenza. L'apertura di tali registri deve essere formalmente e preventivamente richiesta e approvata dal Responsabile della gestione documentale della *AOO* e dal Coordinatore della gestione documentale.

Ciascuna *AOO* può inoltre istituire i seguenti Registri interni:

- Registro atti interni dove vengono registrati i documenti che sono ricevuti o inviati tra Uffici/Utenti della *AOO* (vedi paragrafo 24)

- Registro repertorio dove vengono registrati i documenti legali rilevanti ai fini dell'attività amministrativa della *AOO*, che non siano oggetto di trasmissione/ricezione dalla *AOO*

21. Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:
le gazzette ufficiali, i bollettini ufficiali e notiziari della pubblica *Amministrazione*, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni di natura impersonale (art. 53, comma 5, *testo unico*).

Sono altresì esclusi dalla registrazione di protocollo:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241 e dall'art. 8 del DPR 27 giugno 1992 n. 352, (documenti esclusi dal diritto di accesso)
- i documenti formati all'interno dell'*AOO* e scambiati fra *Utenti*.

Le lettere anonime non sono registrate al protocollo, ma, dopo una preliminare analisi da parte del Consiglio di Presidenza della Giustizia Tributaria, inoltrate, se contengono informazioni o dati di interesse per l'*Amministrazione*, agli *Utenti* di competenza i quali valutano l'opportunità di dare seguito a queste comunicazioni ed individuano le eventuali procedure da sviluppare.
I documenti ricevuti non firmati, per i quali è invece prescritta la sottoscrizione, non sono registrati al protocollo, ma inoltrati agli *Uffici* di competenza i quali individuano le procedure da seguire per risolvere queste situazioni.

22. Registrazione di protocollo dei documenti ricevuti e spediti

Per ogni documento ricevuto o spedito dall'*AOO* è effettuata una registrazione nel Registro Ufficiale di Protocollo o negli eventuali Registri di corrispondenza particolari e autorizzati istituiti dall'*AOO*.
Tale registrazione contiene i dati obbligatori (nucleo minimo di protocollo) che devono essere acquisiti con un'unica operazione, senza possibilità per l'operatore di inserire le informazioni relative al contenuto minimo obbligatorio in più fasi successive (art. 53, comma 3, del *testo unico*). Ogni registrazione di protocollo deve essere univoca e individuare un solo documento.

I dati obbligatori, acquisiti al sistema dagli utenti addetti alle registrazioni di protocollo, sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

- mittente per i documenti ricevuti o, in alternativa, destinatario o destinatari per i documenti spediti (registrazione parzialmente modificabile, tracciata dal sistema con data e autore dell'operazione di modifica);
- oggetto del documento (registrazione parzialmente modificabile, tracciata dal sistema con data e autore dell'operazione di modifica);
- data e numero di protocollo del documento ricevuto, se disponibili;
- impronta del documento informatico associato alla registrazione di protocollo (art. 53, comma 1, lett. f) del *testo unico*) (registrazione parzialmente modificabile, tracciata dal sistema con data e autore dell'operazione di modifica);

Oltre ai dati di carattere obbligatorio suindicati, vengono gestite ulteriori informazioni di carattere accessorio, la cui disponibilità rappresenta una fonte informativa rilevante dal punto di vista amministrativo e organizzativo.

23. Annullamento delle registrazioni di protocollo

E' previsto l'annullamento sia generale che parziale della registrazione di protocollo.

L'annullamento è generale se riguarda l'intera registrazione. Deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile del *SgD* (Allegato 5). Solo il Responsabile del *SgD* è autorizzato a dare disposizioni di annullamento generale delle registrazioni di protocollo.
L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento della intera registrazione di protocollo.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile del *SgD*.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

Si parla di annullamento parziale quando l'annullamento riguarda gli elementi della registrazione classificati come "parzialmente modificabili".

Sia in modalità Ingresso che in modalità Uscita, dopo aver effettuato la protocollazione, è possibile modificare le informazioni sopra citate come "parzialmente modificabili", ovvero annullarne il valore originario sostituendone il contenuto in tutto o in parte, poiché il sistema di protocollo informatico garantisce il tracciamento e la memorizzazione di qualsiasi evento di modifica, tenendo traccia dei nuovi valori inseriti e di quelli originari modificati, della data e dell'ora della modifica e del suo autore (art. 7 e art. 8 delle *Regole tecniche protocollo)*.

E' consentito, inoltre, modificare il documento e gli allegati associati ad una registrazione di protocollo, anche successivamente alla protocollazione, esclusivamente ad un utente che rivesta il ruolo di responsabile del registro.
L'annullamento parziale della protocollazione/registrazione è consentito agli utenti del sistema in possesso dei relativi permessi.

24. Registrazione di protocollo dei documenti interni

I documenti prodotti dagli *Uffici*/*Utenti* della *AOO* che, a giudizio del Responsabile dell'*Ufficio* competente, hanno rilevanza amministrativa vengono registrati esclusivamente sui registri interni:
In questo caso i dati obbligatori sono:

a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) *Utente* che ha prodotto il documento, registrato in forma non modificabile;
d) oggetto del documento (registrazione parzialmente modificabile, tracciata dal sistema con data e autore dell'operazione di modifica.

Per le possibili operazioni di annullamento/modifica si veda il precedente paragrafo 23.

25. Documenti riservati e dati personali

In fase di protocollazione ovvero anche in un momento successivo, qualora il contenuto lo richieda la visibilità di un determinato documento può essere ristretta, qualificando lo stesso mediante l'attributo "Riservato".
Rientra nei compiti del Responsabile del *SgD* la definizione delle tipologie e dei livelli di riservatezza dei documenti. I Responsabili degli *Uffici* del *Consiglio di Presidenza della giustizia tributaria* possono individuare, nell'ambito delle trattazioni di competenza, i documenti a cui applicare determinati livelli di riservatezza in via definitiva o provvisoria, e ne fanno richiesta al Responsabile del *SgD*.

I documenti riservati saranno visibili solo agli utenti autorizzati dal Responsabile del Servizio (vedi Allegato 6)
La protocollazione di documenti riservati è consentita esclusivamente agli utenti ai quali è associato lo specifico ruolo applicativo, con relativo permesso di registrazione. L'operatore di protocollo, quando effettua la registrazione, applica l'attributo "riservato" previsto per il documento in esame.

Per la trattazione dei documenti contenenti dati personali, dati sensibili e dati giudiziari si richiama quanto specificato nella determinazione del Direttore generale delle finanze n. 10291 del 3 maggio 2010 in merito alla designazione dei responsabili del trattamento dei dati personali nelle strutture del DF (vedi Allegato 7).

Secondo quanto previsto dal comma 1 dell'art. 30 del Decreto Legislativo n. 196/2003, ciascuna *AOO* procede all'individuazione nella propria struttura degli incaricati del trattamento dei dati personali, come da schema in Allegato 8).

Rientra nei compiti del Responsabile del *SgD* la definizione delle tipologie di documenti contenenti dati personali e l'individuazione dei documenti per i quali utilizzare l'apposita funzionalità di trattamento dei dati sensibili.

La protocollazione di documenti con dati sensibili è consentita esclusivamente agli utenti ai quali è associato lo specifico ruolo applicativo, con relativo permesso di registrazione. L'operatore di protocollo, quando effettua la registrazione, applica l'attributo "dati sensibili" previsto per il documento in esame.

26. Segnatura di protocollo

La segnatura è l'apposizione o l'associazione all'originale del documento, registrato nei registri di protocollo, in forma permanente non modificabile delle informazioni riguardanti il documento stesso.
L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo e garantisce l'identificazione univoca e certa di ciascun documento.
Le informazioni minime apposte od associate al documento mediante l'operazione di segnatura, ai sensi dell'art. 55 del D.P.R. 445/2000 e dell'art. 9 delle *Regole tecniche PROTOCOLLO*, sono:

codice identificativo dell'*Amministrazione* (nello specifico l'*Ente:* DF*)*
codice identificativo dell'*AOO*
identificativo del Registro;
data di protocollo
progressivo di protocollo

L'operazione di segnatura di protocollo è effettuata dal sistema in modo automatico sui documenti registrati in entrata e pervenuti in forma digitale, e registrati in uscita e formati digitalmente.
L'apposizione della segnatura di protocollo continuerà, invece, ad essere apposta manualmente sui documenti originali cartacei in ingresso o in uscita, al fine di garantire l'associazione univoca tra registrazione di protocollo e originale cartaceo.
L'apposizione manuale della segnatura di protocollo può essere sostituita dall'apposizione della stringatura di protocollo al documento cartaceo mediante l'uso di scanner protocollatori, adeguatamente adibiti a tale operazione.

27. Differimento dei termini di registrazione

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre le quarantotto ore dal ricevimento degli atti.
Eccezionalmente, il Responsabile del *SgD* può autorizzare la registrazione in tempi successivi, fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo.

28. Documenti di competenza di altre amministrazioni

Qualora pervenga all'*Amministrazione* un documento di competenza di un altro *Ente*, ovvero altra *AOO* o altra persona fisica o giuridica, lo stesso viene registrato al protocollo e trasmesso a chi di competenza, se individuabile, altrimenti restituito al mittente, con una lettera di trasmissione opportunamente redatta e protocollata in uscita.

29. Disposizioni particolari sulla ricezione e protocollazione di documenti cartacei

- Documenti inerenti a gare d'appalto

Le offerte inerenti a gare d'appalto, pervenute in forma cartacea, sono registrate al protocollo in busta chiusa. Gli estremi di protocollo sono riportati sulla busta medesima.
Dopo l'apertura delle buste sarà cura della commissione che gestisce la gara d'appalto, riportare gli estremi di protocollo su tutti i documenti in esse contenuti.

- Documenti su supporto cartaceo indirizzati nominativamente al personale dell'Area Organizzativa Omogenea

La posta indirizzata nominativamente al personale dell'*AOO* viene regolarmente aperta e registrata al protocollo dal *SgD,* a meno che sulla busta non sia riportata la dicitura "riservata" o "personale". In questo caso viene recapitata in busta chiusa al destinatario il quale, dopo averla aperta e preso visione del contenuto, se valuta che il documento ricevuto non è personale, lo consegna al *SgD* per la successiva protocollazione (cfr. paragrafo 12 "Ricezione dei documenti su supporto cartaceo").

- Documenti ricevuti prima via fax e, successivamente, in originale su supporto cartaceo

Sono registrati al protocollo i documenti ricevuti via fax, dei quali sia accertata la provenienza, e per i quali non segue la trasmissione cartacea del documento originale (art. 43 del *testo unico*).
Qualora all'*AOO* pervengano successivamente per posta tradizionale gli originali, ad essi saranno attribuiti lo stesso numero e la stessa data di protocollo assegnati ai relativi fax.

- Documenti soggetti a scansione ed uffici abilitati

I documenti ricevuti su supporto cartaceo, di formato inferiore o uguale all'A4 e composti di un numero di pagine inferiore od uguale ad un valore predeterminato dal Responsabile del *SgD*, dopo le operazioni di registrazione e segnatura di protocollo, sono acquisiti in formato immagine mediante l'impiego di scanner.
I documenti di formato superiore all'A4, o composti da un numero di pagine superiore al valore prima menzionato, possono essere acquisiti in formato immagine solo se esplicitamente richiesto dagli *Utenti* di competenza o dal Responsabile del *SgD*.

I documenti con più destinatari sono riprodotti in formato immagine ed inviati di norma solo in formato elettronico.
In ogni caso non vengono riprodotti in formato immagine i seguenti documenti: i certificati medici contenenti la diagnosi; certificati di invalidità; certificati contenenti dati sensibili.

Il Responsabile del *SgD* individua, con l'ausilio dei Responsabili dei procedimenti, gli eventuali ulteriori documenti cartacei da sottrarre al processo di scansione. Per questi documenti egli è tenuto a specificare le modalità ed i tempi, diversi da quelli ordinari, con cui si procederà alla loro digitalizzazione; tuttavia i documenti contabili (fatture, scontrini fiscali e altri documenti assimilabili) presentati unitamente ad istanze volte ad ottenere rimborsi di spese sostenute da parte di Relatori, Consiglieri e Giudici Tributari (nei modi e nelle misure previste con deliberazioni del Comitato) sono allegate alle predette istanze in busta chiusa ed, eventualmente, acquisite in formato immagine solo se esplicitamente richiesto dagli *Utenti* incaricati della trattazione o dei relativi *Responsabili*.

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file in un formato standard abilitato all'archiviazione (tipicamente PDF);
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

N.B.
Le modalità di ricezione e protocollazione dei documenti cartacei illustrate nel presente paragrafo sono destinate a diventare residuali, e comunque esclusivamente ammesse per la ricezione di documenti inviati da mittenti pubblici e privati non soggetti alle prescrizioni del *CAD* e delle *Regole tecniche* (ad es. cittadini privati sprovvisti di identità e indirizzo digitale), mentre tutte le pubbliche amministrazioni soggette al *CAD* entro l'11 agosto 2016 devono adeguarsi allo scambio esclusivo di documenti informatici.

30. Registro di emergenza

Il Responsabile del *SgD* autorizza lo svolgimento delle operazioni di registrazione di protocollo tramite procedura di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura ordinaria. In casi di indisponibilità del *SgD* a livello centralizzato, viene automaticamente attivato il Registro di Emergenza in modalità web.
Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico di cui all'articolo 63 del *Testo unico*.
In particolare:

a) in caso di interruzione della funzionalità del sistema, sul registro di emergenza vanno riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della funzionalità del sistema (operazione non informatizzata, a cura del Responsabile *SgD*);
b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile del *SgD* può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione (operazione non informatizzata, a cura del Responsabile *SgD*);
c) per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente;
d) la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'*AOO*.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, che viene avviata in automatico contestualmente al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
Nel caso in cui i malfunzionamenti del sistema Protocollo fossero tali da non consentire la protocollazione di emergenza via web, il *RgD* autorizza la protocollazione sui Registri di emergenza "stand alone", ovvero presso specifiche postazioni sulle quali è installato l'apposito software.

31. Conservazione dei registri di protocollo

Il Servizio di conservazione dei registri di protocollo si è reso necessario per realizzare l'adeguamento del sistema di Protocollo informatico in uso presso tutte le *AOO* del DF a quanto prescritto dalle *Regole tecniche protocollo* .
Infatti, con riferimento ai requisiti minimi di sicurezza del Sistema di protocollo informatico, l'art. 7 delle *Regole* introduce un importante nuovo obbligo: la conservazione digitale "a norma" del Registro giornaliero di protocollo, definito dal GLOSSARIO allegato alle *Regole tecniche* come il "*registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti*".
Si stabilisce, quindi, che il Registro giornaliero di protocollo sia trasmesso, entro la giornata lavorativa successiva a quella della sua produzione, al Sistema di conservazione, garantendone l'immodificabilità del contenuto.

Per ciascuna *AOO* del presente Manuale sono conservati i seguenti registri giornalieri:

- il Registro Ufficiale giornaliero
- solo i Registri giornalieri di corrispondenza esplicitamente autorizzati
- solo i Registri giornalieri interni esplicitamente autorizzati.

- Contenuto del registro giornaliero di protocollo

Il Registro giornaliero di protocollo comprende, oltre alle informazioni minime richieste dall'art. 53, comma 1, del DPR 445/2000 (numero di protocollo, data di registrazione di protocollo, mittente/destinatario, oggetto, impronta del documento) e dalla Circolare n. 60 del 2013 dell'AgID[4], anche ulteriori informazioni, riportate di seguito, sia per le nuove registrazioni giornaliere di protocollo, sia per le registrazioni in modifica di registrazioni effettuate in date precedenti:

Metadato	**Descrizione**
Numero di protocollo	Numero del protocollo nel formato numero/anno. Es: 00001/2015
Data di protocollo	Data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile
Registro	Indicazione del registro nell'ambito del quale è stata effettuata la registrazione
Modalità	Rappresenta la modalità di protocollazione. Può assumere i valori: I(Ingresso) o U(Uscita)
Mittenti/Destinatari	Rappresenta la lista dei mittenti o destinatari del protocollo. Gli stessi sono proposti sotto forma di elenco come di seguito riportato nell'esempio: Rossi Mario Verdi Antonio; Bianchi Maria
Oggetto	Rappresenta l'oggetto della protocollazione
Data e protocollo ricevuto	Data e protocollo del documento ricevuto, se disponibili;
Impronta Documento Principale	Riporta l'impronta del documento principale, se previsto.
Numero Allegati	Riporta il numero di allegati associati al protocollo.
Allegati e Impronte	Riporta gli allegati del documento principale con le relative impronte
Operatore	Utente che ha effettuato la prima registrazione o che annullato o modificato le informazioni di cui all'art. 53 del *Testo unico*

Tutte le eventuali modifiche effettuate sulle registrazioni di protocollo successivamente alla prima registrazione sono tracciate nel sistema e saranno presenti in una sezione specifica del Registro di protocollo giornaliero.

[4] Circolare n.60 del 2013: Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni;

Di seguito viene riportata una possibile istanza di Registro di protocollo giornaliero, con le due sezioni relative rispettivamente alle prime registrazioni e ai dati relativi alle registrazioni di protocollo modificate.

Dipartimento delle Finanze - AOO di TEST (AOO TEST)
REGISTRO UFFICIALE del 23/09/2015

Nuove registrazioni di protocollo emesse in data 23/09/2015										
Numero di protocollo	Modalità	Data Protocollo	Numero Protocollo Ricevuto	Numero Protocollo Ricevuto	Mittente/Destinatari	Oggetto	Operatore	Impronta documento principale	Numero Allegati	Allegati e impronte
00038/2015	U	23/09/2015			Rossi Mario; Verdi Antonio; Bianchi Maria	Oggetto della protocollazione in uscita	Verdi Mario	g568yh48i5gj4s73	2	Allegato1.pdf - g568yh48i5gj4s73; Allegato2.docx - g589yh12i6gj3d72;
00039/2015	I	23/09/2015	152	22/09/2015	Società di turno spa	Oggetto della protocollazione in ingresso	Rossi Antonio	H123yz14i1gj6s56	2	Allegato1.pdf - g568yh48i5gj4s73; Allegato2.docx - g589yh12i6gj3d72;

Registrazione di protocollo modificate in data 23/09/2015										
Numero di protocollo	Modalità	Data Protocollo	Numero Protocollo Ricevuto	Numero Protocollo Ricevuto	Mittente/Destinatari	Oggetto	Operatore	Impronta documento principale	Numero Allegati	Allegati e impronte
00008/2015	U	21/05/2015			Rossi Amedeo	Oggetto della protocollazione	Bianchi Maurizio		0	
00008/2015	U	21/05/2015			Rossi Amedeo	Oggetto della protocollazione in uscita	Verdi Antonio		0	
00008/2015	U	21/05/2015			Rossi Amedeo	Oggetto della protocollazione in uscita	Verdi Mario	g568yh48i5gj4s73	2	Allegato1.pdf - g568yh48i5gj4s73; Allegato2.docx - g589yh12i6gj3d72;
00019/2015	I	16/06/2015			Azzurro Angelo	Oggetto della protocollazione	Rossi Antonio	g568yh48i5gj4s73	2	Allegato1.pdf - g568yh48i5gj4s73; Allegato2.docx - g589yh12i6gj3d72;
00019/2015	I	16/06/2015			Azzurro Angelo	Oggetto della protocollazione in ingresso	Rossi Antonio	H123yz14i1gj6s56	2	Allegato1.pdf - g568yh48i5gj4s73; Allegato2.docx - g589yh12i6gj3d72;

- Formazione del registro giornaliero di protocollo

Le regole sulla formazione dei registri e repertori informatici sono contenute nell'art. 14 delle *Regole tecniche documento*.
In particolare, il primo comma dell'articolo richiamato stabilisce che il Registro di protocollo è formato ai sensi dell'art. 3, comma 1, lettera d), ossia mediante la "generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica[5]".

Nella fase di formazione del registro giornaliero di protocollo vengono garantite le tre caratteristiche essenziali: la staticità del documento informatico contenente le registrazioni effettuate nell'arco dello stesso giorno, la sua immodificabilità[6] e integrità[7] nel tempo.

[5] Secondo quanto disposto dalle *Regole tecniche* (vedi Allegato 1 – Glossario/Definizioni), la staticità di un documento informatico è rappresentata dalla capacità dello stesso di garantire "*l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione*".

[6] L'immodificabilità è la caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso (vedi Allegato 1 – Glossario/Definizioni delle *Regole tecniche*);

[7] L'integrità è l'insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato (vedi Allegato 1 – Glossario/Definizioni delle *Regole tecniche*);

In particolare, l'art. 3, del DPCM 13.11.2014, al co. 6, stabilisce che nel caso di documento informatico formato ai sensi del comma 1, lettera d), come nel caso di specie, le caratteristiche di immodificabilità e di integrità sono determinate con la produzione di un'estrazione statica dei dati e il trasferimento della stessa nel Sistema di conservazione.

Pertanto, il sistema di Protocollo, per ciascun registro di corrispondenza in stato aperto, ovvero chiuso nella medesima giornata di formazione, definito nel sistema documentale, genera il Registro giornaliero di protocollo, da considerare a tutti gli effetti un documento informatico, quale risultato dell'estrazione statica dei dati contenuti nello stesso sistema di Protocollo, per il quale documento, non sottoscritto con firma digitale, e successivamente trasferito nel sistema di conservazione, sono garantite le caratteristiche di staticità, immodificabilità e intregrità.
Tale documento informatico viene formato tutti i giorni - dopo le ore 24:00 della giornata di riferimento.

- Formato

IL Registro giornaliero di protocollo è prodotto nel formato PDF/A (Portable Document Format) creato per l'archiviazione nel lungo periodo.

Tale formato risulta idoneo alla conservazione in quanto garantisce che il documento assuma le caratteristiche di immodificabilità e di staticità sopra richiamate ed è altresì idoneo a garantire anche la leggibilità[8] del documento nel suo ciclo di vita, cioè assicura che le informazioni in esso contenute siano prontamente disponibili in una forma leggibile su schermo o tramite stampa.

- Sottoscrizione

Il Registro giornaliero di protocollo è generato in via automatica attraverso l'estrazione dal sistema documentale di un insieme di dati, secondo una struttura predeterminata, trasferita in forma statica in un sistema di conservazione, come indicato all'art. 3, comma 1, lettera d), del DPCM 13 novembre 2014.

Tale modalità di formazione del Registro giornaliero di protocollo non rende necessaria la sua sottoscrizione con firma digitale né ai fini di garantirne le caratteristiche di immodificabilità ed integrità né, eventualmente, allo scopo di assicurarne la provenienza e l'autenticità, in quanto il registro di protocollo è comunque riferibile al pubblico ufficiale da cui è formato, cioè il Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo.

- Conservazione digitale del registro giornaliero di protocollo

ll sistema di Protocollo informatico al termine della giornata lavorativa effettua la generazione automatica dei registri di protocollo.

[8] La leggibilità di un documento è data dall'insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti (vedi Allegato 1 – Glossario/Definizioni delle *Regole tecniche*);

Il documento informatico è formato tramite una estrazione statica dei dati contenuti nel sistema di gestione documentale e predisposto con i contenuti descritti in precedenza nel formato richiesto per la conservazione (PDF/A).

I registri giornalieri di protocollo così formati, previsti per il versamento in conservazione, sono inviati automaticamente al sistema di conservazione entro la giornata lavorativa successiva.

Il sistema di conservazione prende in carico i registri di protocollo, verifica la coerenza dei metadati ed effettua le verifiche di formato preliminari alla conservazione dei documenti.
Terminato il processo di conservazione, gli esiti di conservazione ovvero di rifiuto (con relativa motivazione), sono forniti al sistema di Protocollo informatico per la registrazione nei propri archivi.
La durata della conservazione per il documento Registro giornaliero di protocollo è di 30 anni.

- Esibizione dei documenti

Per richiedere l'esibizione del Registro di protocollo di un dato giorno è necessario essere in possesso dell'identificativo, univoco, del documento nel sistema di conservazione.
L'identificativo deve essere recuperato nel sistema produttore del documento, cioè nel sistema di Protocollo informatico, tramite le apposite funzioni a disposizione dell'ufficio.
La richiesta di esibizione, effettuata tramite l'apposita funzione del sistema di conservazione, deve essere richiesta dal personale autorizzato (Responsabile della conservazione o suo delegato).
Il documento potrà essere sarà stampato e il delegato per l'esibizione apporrà timbro e firma per garantirne la conformità.
Sui documenti conservati, in fase di esibizione è disponibile anche la copia del documento con apposto un *watermarke*r che attesta la provenienza del documento dal sistema di conservazione.
Nell'ambito delle operazioni di esibizione è possibile anche accedere agli ulteriori oggetti conservati correlati al documento conservato. Essi sono rappresentati da:

- firmatari del documento, per la verifica delle informazioni di dettaglio;
- lotto di conservazione, per la verifica della composizione del lotto di conservazione;
- marca temporale del lotto di conservazione, per la verifica delle informazioni di dettaglio, ove prevista;
- delega alla firma del lotto, per la verifica dei delegati alla firma dei lotti di conservazione e degli ambiti della delega.

SEZIONE 5 - ASSEGNAZIONE DEI DOCUMENTI

32. Regole di assegnazione

Il *Servizio di gestione documentale (SgD)* di ciascuna *AOO* effettua l'assegnazione dei documenti registrati e/o protocollati in entrata all'*Ufficio*, ovvero agli *Uffici* competenti alla trattazione.
Anche per i documenti in uscita il *SgD* assegna il documento all'*Ufficio* che lo ha prodotto.
Il Responsabile dell'*Ufficio* assegnatario provvede alla trattazione in proprio ovvero riassegnando il documento all'Utente individuato per la trattazione.
E' possibile, per trattazioni specifiche e su indicazione del Direttore o del Dirigente dell'*Ufficio*, assegnare per competenza il documento direttamente all'*Utente* finale.
In ciascuna *AOO* vengono definite eventuali specifiche regole per i documenti che possono/devono essere resi disponibili al Direttore della struttura.
Oltre all'assegnazione per competenza, è possibile l'assegnazione per conoscenza a *Uffici* o *Utenti*.

33. Modifica delle assegnazioni

Nel caso di un'assegnazione ritenuta errata, l'*Ufficio* o *l'Utente* che riceve il documento è tenuto a segnalare il fatto, nel più breve tempo possibile, restituendo, attraverso l'apposita funzionalità prevista nel *Sistema*, il documento all'assegnante che provvederà eventualmente a correggere le informazioni inserite nel *Sistema* e a riassegnare correttamente.
Il *Sistema* di Protocollo informatico tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua l'operazione con la data e l'ora di esecuzione.
E' possibile interrogare il *Sistema*, con ricerca per parole chiave singole o multiple, per individuare gli *Utenti* che stanno trattando, o hanno trattato, un determinato documento.

SEZIONE 6 - ORGANIZZAZIONE ARCHIVISTICA

34. Formazione e gestione dell'archivio corrente

I documenti sono creati, ricevuti e usati dalla *AOO* del presente Manuale a fini pratici e giuridici nell'esercizio delle proprie funzioni istituzionali e devono, quindi, essere gestiti in modo da costituire un supporto funzionale ed efficiente al lavoro d'ufficio

l'archivio è un sistema complesso di documenti in reciproca relazione; in quanto sistema l'archivio deve

- essere unitario(basato su principi di uniformità ricostruibili e conosciuti dai dipendenti)
- essere trasversale a tutto l'ente
- coinvolgere attivamente tutto il personale
- assicurare la continuità della memoria

e utilizza strumenti e metodi di organizzazione dei documenti (il più possibile condivisi e facili da usare): il sistema di classificazione e il piano di fascicolazione

35. Il sistema di classificazione

- Il titolario di classificazione

La classificazione

- è uno strumento di sedimentazione ordinata e razionale per organizzare e ricercare i documenti
- consiste nell'attribuire tutti i documenti prodotti, nel momento della loro formazione e acquisizione, ad una partizione del sistema di classificazione corrispondente alle materie o alle funzioni di competenza dell'amministrazione, al fine di inserire stabilmente i documenti medesimi nella corretta posizione logica e fisica dell'archivio corrente

La classificazione è lo strumento fondamentale per la formazione dell'archivio ed è l'attività finalizzata a identificare e organizzare tutti i documenti, secondo un ordinamento logico, in relazione alle funzioni, alle competenze e alle attività dell'*AOO*.
In ciascuna *AOO* il sistema di classificazione dei documenti è basato su un *titolario di classificazione* e tutti i documenti sono soggetti a classificazione.
Il *titolario* è un sistema logico astratto che organizza i documenti secondo una struttura ad albero, definita sulla base della organizzazione funzionale dell'*AOO*, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.
Il *titolario* è predisposto, verificato e confermato dal Responsabile *SgD* di ciascuna *AOO*. In Allegato 4 sono riportati i *titolari* adottati dalla *AOO* del presente Manuale.
Al momento della pubblicazione del Manuale di gestione, i *titolari di* classificazione vengono contestualmente ufficializzati in quanto presenti in esso.

Mediante la classificazione, si assegna al documento il codice completo dell'indice di classificazione articolato su tre livelli gerarchicamente ordinati: Funzione (1° livello), Macro Processo (2° livello), Processo (3° livello).
Le operazioni di classificazione sono effettuate contestualmente all'operazione di registrazione e segnatura di protocollo.
E' possibile associare al documento più voci di classificazione in relazione alle attività ad esso connesse.
La classificazione può essere modificabile ed integrabile in ogni momento del ciclo di vita del documento

N.B.
Il *titolari*o adottato dalla *AOO* del presente Manuale, riportato nell'Allegato 4, costituisce parte del titolario unico e coordinato dell'Ente Dipartimento delle finanze, che nella sua forma definitiva verrà adottato in concomitanza con l'estensione dei nuovi applicativi realizzati per la gestione del titolario unico centralizzato e per la gestione coordinata dei fascicoli (vedi paragrafo 7).
Il titolario unico centralizzato verrà adottato dal Coordinatore della gestione documentale del DF, con la collaborazione dei Responsabili *SgD* che cureranno l'aggiornamento delle voci di classificazione di pertinenza della propria *AOO*.

- Conservazione e scarto archivistico

I *titolari di classificazione* delle *AOO*, ovvero il *titolario* unico centralizzato del DF, quando verrà implementato, saranno completati anche con l'indicazione dei tempi previsti per l'archiviazione corrente, la conservazione, lo scarto ovvero il versamento all'Archivio di Stato dei documenti e dei fascicoli gestiti dalle *AOO*.

N.B.
L'attività di individuazione dei tempi di conservazione/scarto dovrà essere coerente con il Massimario di conservazione adottato dal MEF per le strutture centrali e con il Massimario di conservazione adottato dalla Direzione Giustizia tributaria per le Commissioni tributarie.

- Tipi di documento

Tutti i documenti protocollati in ingresso ed in uscita possono essere tipizzati, cioè associati ad un "tipo documento", costruito nell'applicativo Protocollo per agevolare e guidare l'acquisizione di un insieme di informazioni, ulteriori rispetto a quelle obbligatorie che costituiscono il "nucleo minimo" di protocollo, che possono essere acquisite dall'Utente protocollatore in fase di registrazione del documento in ingresso ovvero in uscita oppure dall'Utente documentale assegnatario della trattazione del documento.
La tipizzazione dei documenti consente di disporre di un patrimonio di informazioni predefinito, standardizzato, orientato anche a esigenze conoscitive dell'Amministrazione e di reportistica.

- Codificazione dei documenti

La funzione di codificazione dei documenti consente, mediante il dialogo con l'applicativo DSTAXI, l'associazione dei codici di controllo di gestione ai protocolli, al fine di contabilizzare i prodotti del singolo Centro di Costo.
L'associazione della terna "Centro di costo, processo, prodotto" ai protocolli può avvenire in fase di registrazione del protocollo oppure successivamente con l'attività di modifica del protocollo stesso.
La funzione consente quindi di standardizzare le operazioni di acquisizione e successiva estrazione delle informazioni.

36. Il piano di fascicolazione

Poiché la classificazione è finalizzata a sostenere realmente ed efficacemente la sedimentazione delle carte, è necessario che si traduca anche in un vero e proprio piano generale di formazione e gestione del sistema documentario con specifica attenzione per la formazione di fascicoli (piano di fascicolazione), che di norma si aprono in corrispondenza dell'ultimo livello del piano di classificazione.
Pertanto, la classificazione guida la formazione delle aggregazioni documentarie, in modo che tutti i documenti di un fascicolo o di una serie condividono lo stesso indice di classificazione.

- Processo di formazione dei fascicoli

Tutti i documenti ricevuti o prodotti dall'*AOO*, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o pratiche. Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.
Fino all'adozione del *titolario* unico centralizzato e del nuovo applicativo di gestione dei fascicoli, il Responsabile *SgD* di ciascuna *AOO* cura la predisposizione del piano di fascicolazione della propria struttura, integrato e coerente con il *titolario* di classificazione, e tale da contenere l'elenco di tutti i fascicoli della *AOO*, il loro contenuto e l'associazione predeterminata dei fascicoli alle voci di classificazione.

Al fine di assicurare certezza e regolarità al piano di classificazione e fascicolazione, i Responsabili degli *Uffici* curano che sia effettuata la fascicolazione di tutti i documenti di propria competenza. Il Responsabile del *SgD* provvede a verificare periodicamente la correttezza e la completezza delle attività di classificazione e fascicolazione, interessandone, se necessario, i Responsabili degli *Uffici* e curando, su segnalazione degli stessi, l'aggiornamento del piano di fascicolazione contenuto nel *titolario*.
Nell'ipotesi in cui si renda necessario istituire nuovi fascicoli non contemplati dal *titolario*, il Responsabile dell'*Ufficio* di competenza ne fa richiesta al Responsabile del *SgD*, che provvede a verificarne la congruenza con il piano di fascicolazione predefinito dall'*AOO* ed eventualmente ad aggiornarlo.

Tale operazione avviene attraverso l'operazione di "apertura di fascicolo" che consente di registrare nel sistema informatico le seguenti informazioni:

- livelli del *titolario di* classificazione nell'ambito dei quali il fascicolo si collocano;
- numero del fascicolo, generato automaticamente dal sistema informatico;
- nome e descrizione del fascicolo;
- responsabile del fascicolo;
- data di apertura;
- data di chiusura;
- data scadenza;
- stato;
- collocazione fisica, se si tratta di un carteggio;
- lista di competenza associata;
- richiedente (eventuale intestatario del fascicolo);

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento della trattazione. Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Quando si verifica un errore nella assegnazione di un fascicolo, l'*Ufficio* abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel Sistema e ad inviare il fascicolo all'*Ufficio* di competenza.
Il sistema tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore *Utente* che effettua la modifica con la data e l'ora dell'operazione.

In presenza di un documento da inserire in un fascicolo, l'*Utente* abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un affare o procedimento in corso, oppure se ritiene che dia avvio ad una nuova pratica.
Nel primo caso l'*Utente* assegnatario della trattazione assicura l'inserimento fisico del documento nel relativo carteggio; nel secondo richiede l'operazione di apertura del fascicolo al Responsabile del proprio *Ufficio*.

N. B.
L'adozione della nuova componente dei Servizi Documentali per la gestione dei fascicoli renderà necessario rivedere e formalizzare per tutte le *AOO* del DF, ovvero per alcuni gruppi di *AOO,* un sistema comune di regole per la formazione e la gestione dei fascicoli, anche per assicurare l'aderenza alle regole tecniche sui fascicoli informatici, di cui al DPCM 13 novembre 2014.

SEZIONE 7 - PIANO DI SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Nel presente paragrafo si riporta quanto contenuto nel documento QA-23-SD-6Y del 16 Ottobre 2009, versione 1.2 del 16 dicembre 2015 "Misure di Sicurezza specifiche del Sistema di Gestione Documentale" predisposto a cura di Sogei.

37. Descrizione del sistema

- Architettura

Il "Sistema di gestione documentale e protocollo informatico" è una soluzione enterprise che utilizza le seguenti tecnologie:

- J2EE per le componenti di interfaccia e di middleware
- Oracle per la componente DBMS
- EMC Documentum per la componente documentale
- Microsoft .Net per componenti di backend di conversione dei documenti e OCR
- Piattaforme Adobe per la verifica dei formati dei documenti
- Tecnologie ESB per la gestione dei livelli di servizio nell'erogazione di servizi web a disposizione delle applicazioni che producono documenti nei sistemi informativi della varie amministrazioni in cui risiede.

Per facilitare la comprensione dell'intera architettura, si riporta di seguito la component view e la relativa descrizione delle principali componenti.

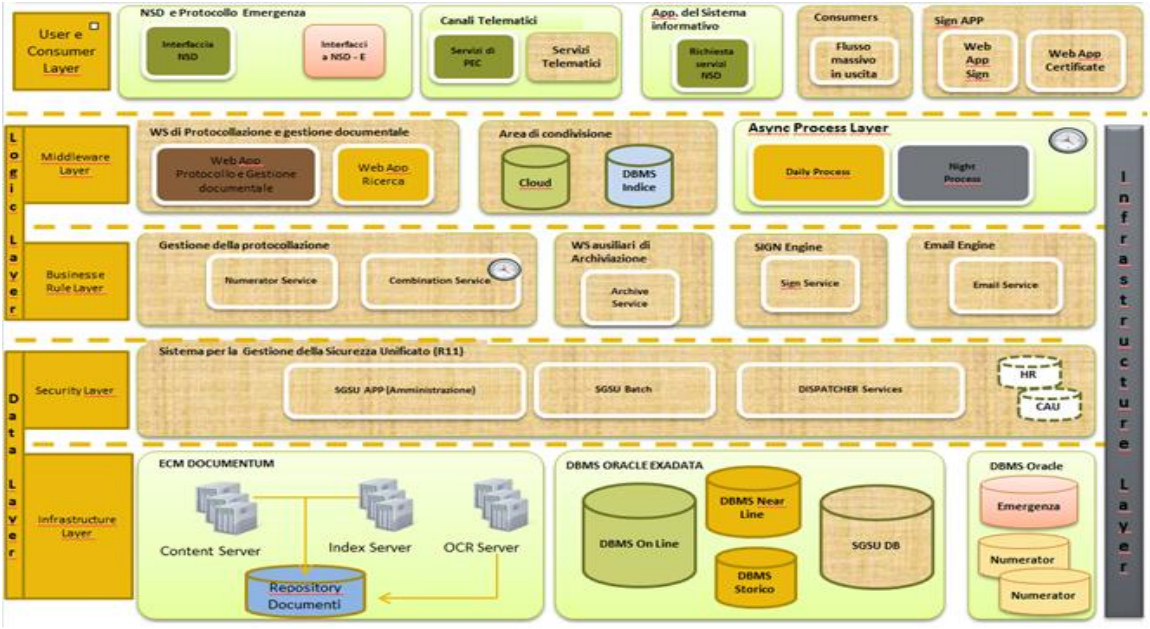

Figura 1 – Component view

- Infrastructure Layer

All' interno dello strato Infrastructure Layer sono incapsulate tutte le componenti di infrastruttura disponibili per l'intera piattaforma di gestione documentale.

  - Authentication Layer: tenuto conto dello scopo di questo documento è opportuno approfondire le componenti relative all'Authentication Layer
    Questo strato è costituito dalle componenti API Active Directory. Le principali funzioni di tale layer riguardano l'implementazione delle azioni scaturenti dai controlli eseguiti tramite l'API Active Directory in fase di identificazione ed autenticazione dell'utente
  - Conversione documenti in PDF: è l'insieme delle componenti hardware e software che permettono di convertire i documenti Office in documenti PDF
  - Verifica della validità della firma digitale dei documenti: è un sistema in grado di accedere alla rete Internet per valutare la validità dei certificati utilizzati per la firma
  - Sistemi di gestione della Posta Elettronica e della Posta Elettronica Certificata

- Componenti applicative

L'architettura del sistema è molto modulare e distribuita su diverse componenti logiche. Le diverse componenti logiche possono essere suddivise nei macro gruppi:

  - User e Consumer Layer
  - Middleware Layer
  - Business e Rule Layer
  - Security Layer
  - Data Layer
  - Componenti Comuni

- User e Consumer Layer

Questo strato applicativo racchiude le componenti che rendono fruibili le funzioni di tutta la piattaforma sia agli utenti, attraverso le interfacce utente, sia ad altre applicazioni, attraverso l'esposizione di servizi web.

Le principali componenti sono:

  - Interfaccia Protocollo: consente di registrare i documenti ai sensi del DPR 445/2000 e del e il DPCM del 13 novembre 2014, assegnare le competenze, classificare e fascicolare i documenti. Attraverso le interfacce di questo strato l'utente assolve alle funzioni di protocollazione, gestione delle attività e fascicolazione di documenti. Oltre a questo espone le funzioni di amministrazione che consentono di rappresentare l'organizzazione degli enti e la profilazione degli utenti. Colloquia con lo strato documentale mediante un "connettore" basato su librerie DFC (Documentum Foundation Classes) e con i Database mediante un adapter applicativo basato su connessioni JDBC. Esiste per questo componente applicativa uno modulo realizzato appositamente per le funzioni di ricerca e reportistica del protocollo informatico che sono più delicate dal punto di vista prestazionale. Rispetto alla componente di protocollazione ha un'architettura applicativa più semplice e interagisce con la stessa mediante delle configurazioni dinamiche.

- Interfaccia Protocollo-E: è un'applicazione WEB che realizza la sola funzione di protocollazione ed è attivata nel momento in cui, a causa di indisponibilità del sistema primario di Protocollo, viene aperta una sessione di emergenza. Colloquia con il database di riferimento mediante un adapter DBMS basato su tecnologia JDBC.
- Servizi PEC: Attraverso gli indirizzi di PEC associati a ciascuna Area Organizzativa Omogenea (AOO), è possibile gestire lo scambio di documenti tra pubbliche amministrazioni e con I cittadini. La soluzione permette di gestire automaticamente più caselle di PEC per ogni AOO offrendo flessibilità nel canalizzare I flussi di documenti scambiati.
- Servizi Telematici: erogati in cooperazione con una nuova infrastruttura di registrazione dei documenti in grado di gestire I carichi dei maggiori flussi di presentazione degli atti da parte dei soggetti interessati, consente di protocollare documenti provenienti da applicazioni utilizzate direttamente dai cittadini.
- Richiesta servizi Protocollo: rappresenta l'interfaccia delle applicazioni verso i servizi del Protocollo. Tipicamente sono applicazioni che attraverso i servizi effettuano le seguenti operazioni: archiviazione e ricerca documenti, oppure generazione e ricerca protocolli
- Flusso massivo in uscita: Rappresenta un canale ad uso di applicazioni che richiedono la protocollazione massiva di documenti prodotti in modalità bach da inviare ad una moltitudine di soggetti. Sono correlate a ciò l'archiviazione, la firma e la spedizione massiva di documenti.
- Firma : consente di firmare singoli documenti o un gruppo di documenti in un'unica sessione (basket) utilizzando smart card o sistemi di firma remota. E' una componente web con la quale si gestiscono in maniera trasversale le problematiche inerenti la firma digitale dei documenti. Attraverso questo strato gli utenti possono firmare documenti o accedere alle informazioni che certificano documenti già firmati da altri
- Web App Certificate: abilita o meno l'utilizzo del certificato di firma in modalità remota-massiva

- Middleware Layer

Questo strato include tutte le componenti che espongono le funzioni di business dell'intera soluzione.

Le principali componenti sono:

- WS di protocollazione e gestione documentale: rappresenta il catalogo dei servizi web adeguati al sistema di gestione della sicurezza unificato (Amministrazione - SGSU). Ciò consente di applicare le policies di accesso alle risorse documentali (Documenti e Fascicoli) dell'utente che sta eseguendo l'operazione rispetto al ruolo ricoperto nell'organizzazione. In tal modo l'accesso alle risorse documentali è garantito dall'infrastruttura del sistema documentale indipendentemente dal contesto operativo in cui si trova ad operare l'utente. In altri termini l'utente può accedere alle risorse documentali se ne ha il privilegio indipendentemente dall'applicazione che sta utilizzando.
- Area di condivisione dei documenti: è concettualmente concepita come un'estensione logica e fisica dei livelli di visibilità associati ad un protocollo, sia esso in ingresso o in uscita. Costituisce uno strumento attraverso il quale le figure interessate ai protocolli

possano consultare i relativi dati e documenti al di fuori del perimetro dell'Area Organizzativa Omogenea (AOO) di riferimento.

- Async Process Layer: È l'insieme dei processi asincroni correlati alla gestione dei documenti scambiati o alla corretta applicazione delle regole di gestione del sistema di protocollazione. Con "Daily Process" si intendono i processi le cui elaborazioni sono schedulate in continuità durante il giorno per gestire i messaggi di PEC e PEL (interoperabilità) e per archiviare i documenti scambiati mediante i servizi telematici. Per "Night Process" sono processi con schedulazione unica nell'arco della notte e si occupano di gestire i registri di protocollazione, farne la stampa giornaliera ed effettuare attività di controllo e quadratura.
  Di seguito viene effettuato un approfondimento sui due gruppi di processi.

  Processi asincroni (Daemon) a schedulazione giornaliera (frequente):
  - Stampe in Differita: processo asincrono che crea e salva su documentale i report in pdf ed Excel richiesti dagli utenti mediante l'applicazione Web protocolloASP. Le stampe non vengono create dall'applicazione online a causa del volume di dati eccessivo che devono essere estratti, che potrebbe compromettere le prestazioni dell'applicazione stessa. Il valore di soglia è configurabile per ente.
  - Ricerche Asincrone: è un processo asincrono costantemente in "ascolto" di richieste di consultazioni dati particolarmente pesanti per la mole di informazioni che si vanno ad elaborare. Si occupa dell'esecuzione della richiesta e della predisposizione dei risultati.
  - Controllo utenti collegati: processo asincrono che controlla la sessione applicativa degli utenti del Protocollo e invalida quelle inattive da un periodo stabilito è configurabile per ente.
  - Aggiorna Campi Denormalizzati: esegue la denormalizzazione dei dati del protocollo informatico necessaria per rendere prestazionalmente più efficienti alcune query sui database.
  - Mail download MPEC: processo asincrono che scarica i messaggi dalle le caselle di posta configurate per il protocollo informatico.
  - Mail invio MPEC: processo asincrono che invia le email in uscita dal sistema di protocollo al sistema di PEC.
  - Mail elabora MPEC: processo asincrono che elabora, sbustando e spacchettando le mail scaricate dalle caselle di posta certificata configurate per il protocollo informatico. Eventualmente classifica le mail come ricevute di PEC associandole ai protocolli in uscita che le hanno originate.
  - Telematico: processo asincrono che elabora i documenti inviati attraverso il canale telematico e provvede quindi attraverso una fase di validazione del formato a scartarli o accettarli e quindi associarli al protocollo precedentemente emesso e ad assegnarlo al funzionario o struttura competente per la lavorazione.
  - CDR - Control Data Recovery: si tratta della componenti software introdotte per garantire sempre un corretto allineamento tra i protocolli emessi nell'archivio del DBMS del Numerator Layer e l'archivio dell'applicazione Protocollo

  Processi asincroni (Daemon) a schedulazione notturna (unica nelle 24 ore):

- Stampe in Differita Complete: processo asincrono che realizza la stessa funzionalità del processo asincrono "Stampe in Differita" ma che per ogni elemento atomico estrae ancora più dati per cui viene eseguito solo in momenti di poco carico dei database (tipicamente tardo pomeriggi e notte)
- Gestione Registri: chiusura e apertura dei registri attivi del protocollo informatico. Viene eseguito alle 00.00 di ogni giorno e apre alla data odierna i registri che erano aperti anche il giorno precedente. Può essere eseguito solo una volta al giorno.
- Gestione Stampa Registri: crea la stampa PDF giornaliera dei registri del protocollo informatico e ne salva l'identificativo documentale sui database.
- Storicizzazione Uffici: processo asincrono che verifica la possibilità di esecuzione di una storicizzazione di un ufficio pianificata ed esegue quelle verificate e pianificate per la data odierna.
- Aggiorna dati del Protocollo di emergenza: processo asincrono che sincronizza i dati di amministrazione e organizzazione dai database degli enti a quello di emergenza.
- Import Emergenza Protocollo: processo asincrono che importa e protocolla i protocolli registrati con l'applicazione Protocollo Emergenza Web.
- Storicizzazione dati: processo asincrono che esegue il trasferimento dei dati considerati "storicizzabili" secondo alcune regole dinamiche. La storicizzazione sposta i dati dal database corrente al database storico in base a dei parametri configurabili per ente.
- SGSU Batch: è una componente JAVA che ha lo scopo di far conoscere all'infrastruttura documentale le strutture organizzative derivate dal sistema HR. Questo si realizza attraverso una procedura batch che recupera dal sistema HR di Sogei le informazioni necessarie e le riporta nell'ambito del repository LDAP del CAU. L'output di questa componente è la creazione di gruppi e ruoli che saranno utilizzati nella generazione delle ACL dei documenti e dei fascicoli.

Tutti i processi asincroni sono installati e schedulati su due server dedicati in modo da garantire il servizio anche in caso di indisponibilità di uno dei due server. Un meccanismo a semafori impedisce l'esecuzione contemporanea di due istanze dello stesso processo asincrono. Alcuni invece permettono l'esecuzione in parallelo (multithreading).
Rispetto ai processi sopra riportati, è importante sottolineare che esistono dei sistema di controllo, che periodicamente, durante le 24 ore, effettuano delle verifiche per individuare eventuali blocchi o malfunzionamenti. In tali casi, provvedono ad inviare delle email di notifica ad una casella funzionale presidiata da personale preposto.

- Business e Rule Layer

Le componenti di questo strato applicano le regole di business inerenti la protocollazione e la gestione dei documenti.

- Gestione della protocollazione: rappresenta la componente infrastrutturale e centrale del sistema di protocollazione. Infatti , nell'ambito del modello architetturale ha il compito di generare la segnatura di protocollo nel pieno rispetto del DPCM del 31 ottobre 2000 a fronte delle richieste di registrazioni effettuate tramite Protocollo, i

servizi telematici, i consumer ITC e le applicazioni del sistema informativo. E' costituito dalle due seguenti componenti:

- Numerator Services: sono i servizi che hanno lo scopo di generare la segnatura di protocollo richiesto dai vari consumer. E' la componente del sistema che deve garantire i maggiori livelli di performance; per tale motivo la sua architettura è scalabile in relazione ai picchi e ai carichi transazionali attesi.
- Combination Services: sono i servizi che hanno lo scopo di abbinare e archiviare i documenti associati a ciascuna segnatura di protocollo emessa attraverso il Numerator Service.
- Archive Service: il catalogo dei servizi per l'archiviazione massiva di documenti da sottoporre alle fasi successive di lavorazione come ad esempio la firma digitale, la successiva protocollazione e spedizione.
- Sign Service: è la componente unica che attua la firma digitale dei documenti nelle modalità:
  -Smart Card per la firma di un solo documento o di un gruppo di documenti (basket).
  -Sistemi per la firma di un solo documento o di un gruppo di documenti (basket) utilizzando la firma remota.
  -Firma Remota Automatica per la firma massiva di documenti.
- Email Service: è la componente di colloquio con i sistemi di PEC e PEL per la gestione di messaggi di posta. Sono utilizzati i protocolli POP e SMTP per interagire con i sistemi di posta.

- Security Layer

E' lo strato che applica le politiche di sicurezza sulle risorse documentali, i documenti e io fascicoli derivate dalla collocazione di ciascun utente nella struttura organizzativa di appartenenza e/o in base a specifiche esigenze (ad. esempio l'appartenenza a gruppi di lavoro).
Le regole di visibilità e di accesso alle risorse documentali sono attuate mediante la creazione di specifiche ACL (Access Control List) per ciascun documento o fascicolo.
E' costituito da tre moduli fondamentali:

- Amministrazione SGSU -APP: è una web app che permette di definire particolari ruoli da associare agli utenti derivanti dai contesti operativi piuttosto che dalla struttura di appartenenza degli utenti. Un esempio di ruolo «applicativo» è l'attribuzione dei permessi di protocollazione
- SGSU BATCH: è una componente JAVA che ha lo scopo di comunicare all'infrastruttura documentale le strutture organizzative derivate dal sistema HR e riportate sull'LDAP del CAU tramite una procedura batch. L'output di questa componente è la creazione di gruppi e ruoli che saranno utilizzati nella generazione delle ACL dei documenti e dei fascicoli
- Dispatcher Services: è la componente software che si occupa di applicare ad ogni singola risorsa documentale le regole di sicurezza definite in base alla risorsa documentale e al processo applicativo nel quel è coinvolta. Obiettivo di questa componente è l'aggiornamento delle ACL dei documenti e dei fascicoli per modificare le politiche di accesso dei documenti e fascicoli in relazione al flusso di lavorazione.

- Data Layer

All'interno di questo strato risiedono tutte le componenti della architettura che rendono persistenti le informazioni, siano essi documenti o dati elementari.
E' costituito dalle seguenti componenti:

  - EMC Documentum: è un'istanza di una installazione della piattaforma EMC Documentum. Rappresenta lo strato comune a tutte le componenti applicative, a cui è demandata l'attuazione delle politiche di sicurezza rispetto alle ACL di ciascuna risorsa documentale. E' costituito dalle seguenti componenti:
  - Repository Documenti: È costituito da diversi DOCBASE (uno per ogni ente) ed è il repository dei documenti. È costituito da due database uno che contiene i metadati dei documenti e uno necessario per le informazioni di indicizzazione.
  - Content Server: sono l'insieme delle componenti hardware e software che gestiscono l'accesso e le elaborazioni sul Repository
  - Index Server: sono le componenti hardware e software dedicate all'indicizzazione dei documenti per agevolare le ricerche di tipo FULL TEXT
  - OCR Server: sono le componenti hardware e software dedicati alla scansione e riconoscimento ottico dei documenti e alla relativa archiviazione
  - DBMS ORACLE EXDATA: si tratta di una istanza ORACLE 11 implementato su piattaforma EXADATA. I DBMS di cui è costituito sono i seguenti:
  - DBMS On Line: sono presenti in questo archivio i dati relativi alla protocollazione, alla gestione delle attività e ai fascicoli. Esiste uno schema per ogni ente.
  - DBMS Near Line: sono presenti le stesse tipologie di informazioni dell'archivio on Line, ma si riferiscono a documenti per i quali è stata completata la lavorazione. La presenza di questo archivio rende maggiormente performante l'archivio on line. Anche per questo strato esiste uno schema per ogni ente
  - DBMS Storico: nell'archivio sono presenti i dati dei protocolli precedentemente utilizzanti dalle AOO prima dell'attivazione di Protocollo. Anche per questo strato esiste uno schema per ogni ente
  - SGSU DB: è l'archivio in cui vengono rappresentati le strutture organizzative presenti in HR e nel CAU.
  - DBMS Emergenza: Sono presenti i dati dei protocolli emessi durante la fase di emergenza. E' un DBMS che nel momento in cui viene ripristinato il servizio Protocollo viene svuotato dei suoi dati che sono sincronizzati sul DBMS On Line dello strato DBMS Oracle Exadata.
  - Numerator: si tratta di una base di dati dedicata, ovvero che ha il solo scopo di generare il numero di protocollo secondo il formato della segnatura di protocollo. Viene ridondato in alta affidabilità al fine di garantire la massima tenuta in termini di fault – tollerance in caso di guasti.

- Componenti Comuni

Quanto precedentemente rappresentato, fa uso di alcune componenti che possono definirsi comuni in quanto utilizzate da tutti i layer della piattaforma di seguito elencati.

- Acquisizione massiva: realizza la funzionalità di acquisizione massiva che permette di elaborare i documenti messi a disposizione dallo strato documentale "CAPTIVA"(OCR).
- Connettore DFC: libreria java standard che espone dei metodi di colloquio con il sistema documentale basato sulle API messe a disposizione da EMC Documentum. E' utilizzato da tutti gli altri componenti applicativi per colloquiare con il documentale.

- DATI TRATTATI

I dati memorizzati nel sistema sono costituiti da:

- Protocollo - Utenti" – Sono gli utenti che associati a determinati uffici di un Area Organizzativa Omogenea e opportunamente profilati in base a ruoli/permessi accedono al sistema Protocollo. Un Area Organizzativa Omogenea è un insieme definito di unità organizzative di una amministrazione, che usufruisce, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali.
- Protocollo – Documenti Informatici" - Sono i documenti informatici acquisiti sia attraverso la protocollazione che direttamente inseriti nei fascicoli elettronici.
- Protocollo – Protocolli Attività" - Sono le registrazioni effettuate su un determinato registro di protocollo di una AOO. Comprende anche le registrazioni effettuate sul registro di emergenza di un'AOO quando il sistema Protocollo non è disponibile, secondo quanto stabilito dall'art.63 del DPR 445/2000. Le attività comprendono le operazione che tracciano il flusso relativo a protocolli, registrazioni, tra le attività sono compresi anche gli eventi che tracciano le operazione significative effettuate dagli utenti.
- Protocollo – Fascicoli" – rappresentano un aggregazione strutturata ed univocamente identificata di documenti o documenti informatici prodotti e funzionali allo svolgimento di una specifica pratica amministrativa.

I dati strutturati e di identificazione sono memorizzati nel DB Oracle, mentre i relativi documenti ed eventuali fascicoli sono memorizzati nel sistema documentale EMC Documentum.

38. Sicurezza del servizio

-IDENTIFICAZIONE DEGLI UTENTI

Gli utenti del servizio sono dipendenti della Sogei e come tali censiti nel dominio AD denominato DOMUS con interfaccia Active Directory; pertanto rientrano nella sua infrastruttura di gestione centralizzata.

-AUTENTICAZIONE DEGLI UTENTI

L'applicazione, all'atto dell'accesso di un utente, ne verifica le credenziali (user-id e password) interrogando il sistema di autenticazione Active Directory di DOMUS sul quale sono censiti i dipendenti Sogei. Le policy di sicurezza degli utenti (eventuale revoca, criteri di complessità e periodo di validità delle password, ecc.) sono gestiti dall'infrastruttura centrale e da tale interfaccia Active Directory, con opportuni parametri di scambio, comunica all'applicazione eventuali

informazioni aggiuntive rispetto alla semplice verifica della password inserita in fase di autenticazione.

-GESTIONE DEGLI UTENTI

L'amministrazione degli utenti avviene attraverso i workflow di autorizzazione e le interfacce di controllo. Gli amministratori sono censiti e gestiti all'interno dell'infrastruttura attraverso un sistema gerarchico di deleghe. Gli utenti sono gestiti in base ad ambiti di visibilità – definiti da requisiti applicativi – di ciascun amministratore, e vengono da questi abilitati all'applicazione specifica.

-GESTIONE DELLE AUTORIZZAZIONI

Per motivi di astrazione rispetto ai criteri di autorizzazione specifici di ogni ente utilizzatore del sistema, è stato stabilito di gestire i profili utente di Protocollo all'interno dell'applicazione Amministrazione.
Il sistema implementa criteri organizzativi di sicurezza proponendo una struttura organizzativa preordinata, basata sul principio di separazione dei ruoli e delle relative responsabilità operative.
Esso prevede infatti i seguenti ruoli applicativi di base per ogni Ente:

- ✓ Amministratore di Ente (di seguito Amministratore)
- ✓ Amministratore di Area Organizzativa Omogenea (di seguito AOO)
- ✓ Utente (classe di utenza che opera prevalentemente sui fascicoli)
- ✓ Operatore (classe di utenza che opera prevalentemente sui protocolli)

Oltre questi ruoli base, ogni Ente può definire nuovi profili utilizzando una qualsiasi combinazione dei permessi previsti dal sistema.

In ottemperanza al principio di segregazione di ruoli e responsabilità, i suddetti profili in Protocollo sono associati alle seguenti operazioni/risorse:

- Amministratore:
  - Amministrazione di Ente (parametri di configurazione, AOO, ruoli, uffici, utenti, tipi documento)
- Amministratore di AOO:
  - Amministrazione di AOO (associazione ruoli – utenti – uffici, tipi documento).
  - Chiusura registri
  - Modifica titolario
  - Chiusura annuale registri
  - Autorizzazione all'installazione dei sender
  - Controllo attività di acquisizione massiva
  - Crea/Modifica tipi di attività
  - Gestione utenti non associati all'AOO
  - Modifica registri
  - Apertura registri
  - Creazione e modifica dei report
  - Modifica mezzi di spedizione
  - Modifica categorie persone giuridiche
  - Responsabile servizio di emergenza

- Utente:
    - Impostazione lista di competenza
    - Creazione/Modifica fascicoli
    - Assegnazione per conoscenza in una pratica
    - Autorizzazione dati sensibili
    - Gestione documenti con dati sensibili
    - Lettura registri
    - Lettura registri limitata
    - Gestione dossier
    - Accesso ai fascicoli Esecuzione reports
    - Gestione scadenze ufficio
    - Riapertura dei fascicoli chiusi
    - Ricerca per ufficio mittente
    - Crea/Modifica tipi di attività
    - Modifica dei campi estesi
    - Utente documentale
    - Consultazione/Richiesta import pregressi
    - Creazione attività
    - Controllo procedimenti
    - Riapertura procedimenti
- Operatore:
    - Annullamento protocollazione
    - Modifica rubrica
    - Protocollazione in ingresso
    - Eliminazione check dati sensibili
    - Eliminazione check riservato
    - Esecuzione import protocolli pregressi
    - Protocollazione in uscita
    - Protocollazione riservata
    - Registrazione
    - Modifica oggettario
    - Protocollazione in entrata da casella istituzionale
    - Gestione degli elenchi di spedizione
    - Annullamento parziale
    - Gestione delle spedizioni dei protocolli
    - Inserimento mittente/destinatario giuridico libero
    - Gestione import pregressi

Con l'integrazione all'infrastruttura alla versione R11 è necessario profilare gli utenti anche dal punto di vista dell'organizzazione di cui fanno parte in HR.
Anche sul sistema di Amministrazione- SGSU sono previsti i ruoli di amministratore, amministratore di AOO e amministratore di Ufficio, che possono operare associando agli utenti i ruoli organizzativi nell'ambito di ogni ufficio delle AOO, che sono:

- responsabile
- facente funzione
- Segreteria

Nell'ambito di ogni ufficio devono essere individuati i "protocollatori".
Sempre in Amministrazione-SGSU è prevista l'attribuzione del ruolo applicativo per poter gestire sia i documenti riservati che i documenti con dati sensibili nell'ambito dell'AOO di appartenenza.
Le profilature effettuate in Amministrazione-SGSU andranno a costituire i relativi gruppi di utenti sulla piattaforma documentale e serviranno a garantire la sicurezza sui documenti e sui fascicoli attraverso il meccanismo delle ACL (Access Control List).

-Visibilità sugli oggetti documentali

La visibilità sugli oggetti documentali, documenti e fascicoli, è gestita attraverso la nuova versione R11 della Piattaforma .
La versione R11 è la piattaforma infrastrutturale che applica le politiche delle ACL per ciascun documento o fascicolo.
In tal modo sicurezza sulle risorse documentali, documenti e fascicoli, derivate dalla collocazione di ciascun utente nella struttura organizzativa di appartenenza e/o in base a specifiche esigenze (ad. esempio l'appartenenza a gruppi di lavoro).
Le regole di visibilità e di accesso alle risorse documentali sono attuate mediante la creazione di specifiche ACL la visibilità e l'accesso a ciascun documento o fascicolo sono garantiti dai servizi nativi dell'infrastruttura documentale indipendentemente dal contesto operativo utilizzato dall'utente per accedere ai documenti o ai fascicoli.
Per l'attuazione di questo modello è vincolante la conformità dei consumer alle modalità di determinazione dei privilegi di ciascun utente e alle regole di creazione ed aggiornamento delle suddette ACL.
Rappresenta un veicolo fondamentale per la condivisione sicura e controllata dei documenti e dei fascicoli durante le fasi di lavorazione di distinti processi amministrativi tra loro correlati e dipendenti
E' costituito da tre moduli fondamentali SGSU APP, SGSU BATCH e Dispatcher Service già menzionate nella porzione architetturale: Flussi ruoli / risorse
Di seguito viene riportato uno schema per ciascun ruolo, in cui si mostrano i diversi flussi dei dati, le relazioni tra i profili e tra i diversi permessi previsti nell'applicazione. Ogni schema descrive la sequenza delle attività dei vari ruoli e le eventuali relazioni tra di loro.

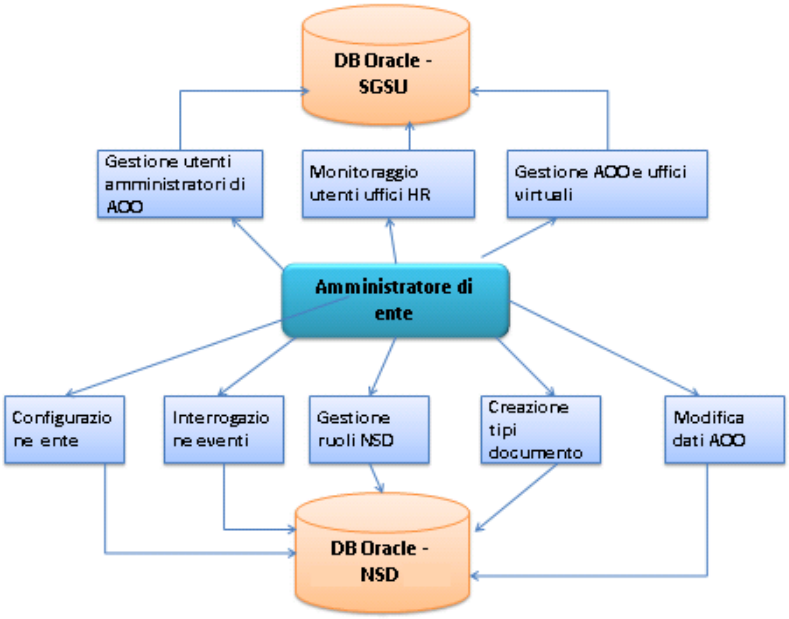

Figura 2 - Amministratore di ente

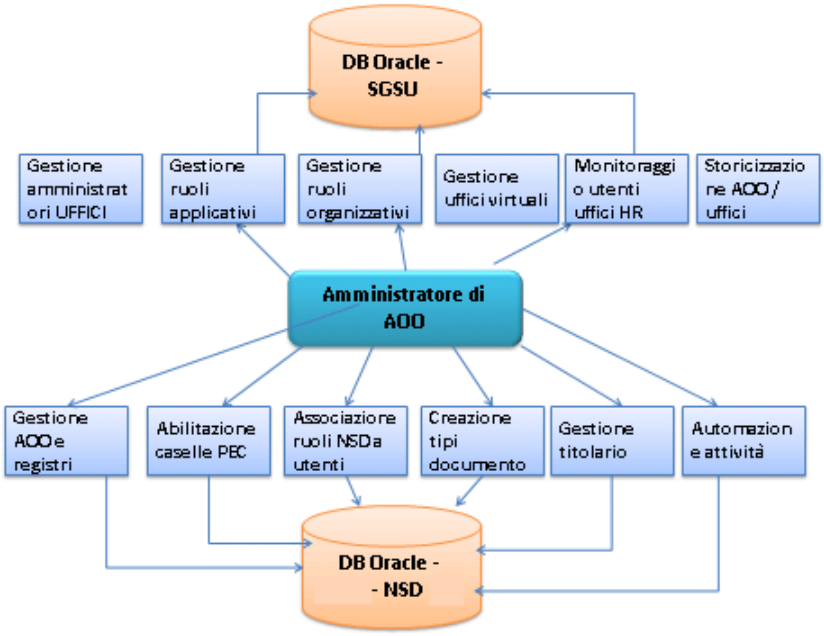

Figura 3 - Amministratore di AOO

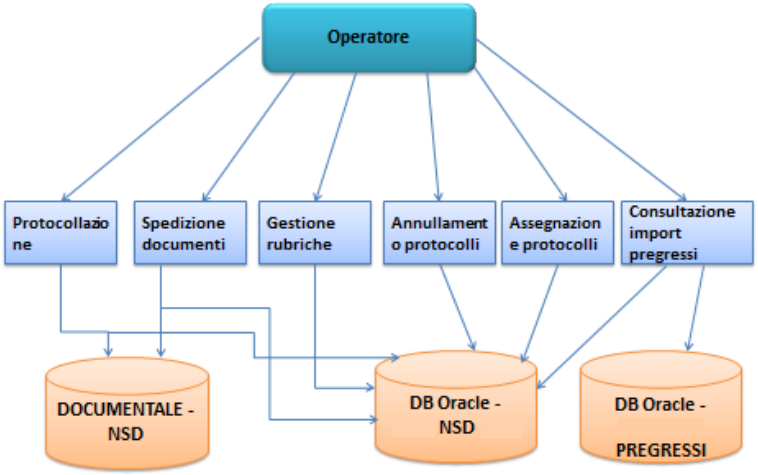

Figura 4 – Operatore

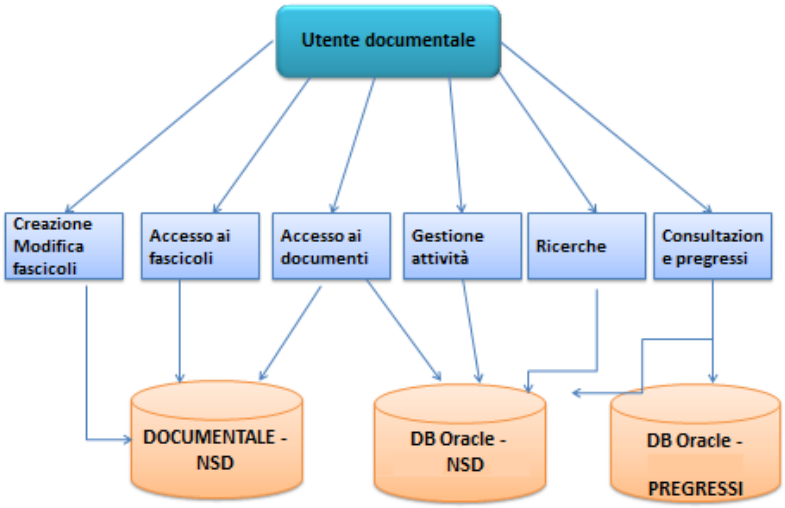

Figura 5 – Utente

-TRACCIAMENTO DELLE OPERAZIONI

Le operazioni effettuate dagli utenti sono tracciate all'interno di archivi dedicati.
Periodicamente queste informazioni sono rimosse dal database operazionale e trasferite in archivio storico ma sempre consultabile dagli utenti finali che ne hanno il permesso.
Tutte le operazioni di amministrazione degli utenti effettuate attraverso le interfacce standard di CAU sono tracciate con estrema granularità dall'infrastruttura stessa.
Le uniche operazioni di amministrazione che sono tracciate sono quelle relative alla gestione delle credenziali dell'utente in Active Directory e comprendono anche le operazioni di login e logout.

-GESTIONE DI LOG APPLICATIVI

Tutte le operazioni effettuate tramite il sistema vengono tracciate mediante log applicativi, dalla fase di accesso al sistema (login) alla fase di disconnessione (logout).
I tracciamenti delle operazioni sono effettuati sia per gli utenti sia per le applicazioni consumer che interagiscono attraverso il servizi infrastrutturali documentali.
I log sono archiviati su file system e alcuni di essi registrati anche in una tabella interna all'applicazione, con riferimento alle operazioni di inserimento, modifica di una struttura, di protocollazione o di gestione di documenti.
Di seguito i dati più significativi:

- DATA_EVENTO: data e ora in cui si è generato l'evento
- DESC_SHORT_AUTORE: UserId
- DESC_OGGETTO: segnatura
- DESC_TIPO_OPERAZIONE: tipologia dell'operazione effettuata (login, creazione Id, protocollazione, etc)
- DESC_DESCRIZIONE: descrizione operazione effettuata
- STAT_TIPO_EVENTO: Descrizione statistica della tipologia delle operazioni più comunemente effettuate
- DESC_TIPO_OGGETTO: Nome della classe Java invocata dall'operazione
- Per maggior chiarezza, si riporta un esempio della registrazione dei log

STAT_TIPO_EVENTO
Amministrazione
Protocollazione
Documentale

STAT_OGGETTO
SpeedCopiaDocProto
SpeedRuolo
SpeedAnnoRegistro
SpeedPratica
SpeedNodoTitolario
SpeedNodoGruppoIndirizzo
SpeedUfficio
SpeedProfiloDocProto
SpeedUtente
SpeedAoo
SpeedFolder

DESC_TIPO_OPERAZIONE
Creazione ufficio
Modifica permessi registro
Protocollazione in uscita
Protocollazione in ingresso
Cancella registro
Modifica ruolo
Visualizza documento
Modifica pratica
Cancellazione cartella
Cancella pratica
Modifica ACL pratica
Stampa timbro
Chiusura registro in uscita
Cancella ufficio
Cancella acl
Apertura registro in ingresso
PROTOCOLLAZIONE
Modifica protocollazione uscita
Rinomina cartella
Cancella nodo titolario
Creazione utente
Login
Creazione aoo
Creazione ruolo
Presa in carico
Creazione cartella
Cancellazione assegnazione documento
Annullamento protocollazione ingresso
Cambio anno riferimento registro
Modifica acl
Disabilitazione utente
Riassegnazione documento
Riapertura pratica
Modifica ufficio
Modifica nodo titolario
Creazione registro
Modifica protocollazione ingresso
Annullamento protocollazione uscita
Modifica casella istituzionale
Logout
Creazione acl
Apertura registro in uscita

DESC_TIPO_OPERAZIONE
Classificazione documento
Assegnazione documento
Creazione pratica
Cancella ruolo
Creazione nodo gruppo indirizzi
Cancella nodo titolario gruppo indirizzi
Modifica aoo
Modifica utente
Acquisizione documento
Chiusura registro in ingresso
Cancella folder
Rifiuto assegnazione
Taglia documento
Upload documento
Chiusura pratica
Download documento
Creazione nodo titolario
Modifica ACL documento

Il salvataggio delle componenti Oracle, vengono garantite dai meccanismi di backup dell'intera istanza del DB.

-LOG IN RELATIVI ALLE ISTANZE WAS

Applicazione Protocollo

L'applicativo web e i servizi web utilizzano come file di logging applicativo lo Speed-log.txt archiviato nel file system degli application server WAS nel path:

/prod/installedApps/speedWebsphere/logs

Inoltre, vengono anche utilizzati i files di log tipici dell'istanza WAS SystemOut.log archiviati nel path (per ognuno dei membri del cluster) su:

/prod/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/protocolloWS_P0xCL

Componenti relative al Numerator Layer

Relativamente al nuovo strato relativo al Numerator Layer tutte le componenti utilizzano come file di logging applicativo il CDR-log.txt archiviato nel file system degli application server WAS nel path:

/prod/installedApps/CDR/logs

Inoltre, vengono anche utilizzati i files di log tipici dell'istanza WAS SystemOut.log archiviati nel path (per ognuno dei membri del cluster) su:

/prod/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/

-LOG DEI PROCESSI ASINCRONI

Per tutti processi asincroni i file di log applicativi sono tracciati nel file system del server dedicato a tali processi nel path:

/prod/app_speed/temp

-LOG RELATIVI AI FRONT END HTTP

Relativamente agli accessi ai front-end di accoglienza, sono presenti sui server http gli access-log al seguente path:

/prod/IBM/HTTPServer/logs

-LOG RELATIVI AI MECCANISMI DI INTEROPERABILITA'

Relativamente ai meccanismi di interoperabilità, i log relativi alle trasmissioni effettuate dai sistemi di PEC e PEL, non sono memorizzati negli archivi o nei file system dell'applicativo Protocollo, ma sono conservati direttamente sulle piattaforme di gestione della posta.

-STORICIZZAZIONE DEI LOG

Tutte le categorie di log sopra rappresentate sono conservati a vita in doppia copia su nastro. Non sono disponibili online in quanto la procedura di storicizzazione provvede alla rimozione dai sistemi.

Il recupero di tali log in caso di necessità avviene tramite richiesta (e-mail) alla struttura tecnica di competenza, che provvederà a rendere ispezionabile una copia dei dati in un'area di appoggio momentanea.

-MODALITÀ DI CONSERVAZIONE DEI LOG

I log indicati di seguito sono conservati a vita in doppia copia su nastro, non sono disponibili online in quanto la procedura di storicizzazione provvede alla rimozione dai sistemi:

- log applicative: speed-log
- log degli accessi dell'applicazione firma e verifica
- log degli accessi degli http di front-end
- log applicativi del CDR (Control Data Recovery)

Il recupero di tali log in caso di necessità avviene tramite richiesta (e-mail) alla struttura tecnica di competenza, che provvederà a rendere ispezionabile una copia dei dati in un'area di appoggio momentanea.

-MODALITÀ DI GESTIONE DEGLI ERRORI

Applicazione Protocollo e servizi web di gestione documentale

La gestione degli errori si compone di due aspetti. Il primo riguarda il tracciamento degli eventi e dei dati all'instante dell'errore, il secondo riguarda la notifica agli utenti. Nel primo caso sono utilizzati prevalentemente i meccanismi di logging dei sistemi, nel secondo caso è fornito un messaggio all'utente finale del sistema.

In particolare, durante il flusso di protocollazione di un documento e le successive fasi di lavorazione, il sistema provvede all'inserimento dei dati nell'apposito DB relazionale e all'archiviazione del documento nel sistema documentale con la tracciatura degli errori nei LOG applicativi e di sistema e con messaggi di risposta all'utente.

Nel caso specifico di errore in fase di archiviazione del documento nel sistema documentale, il sistema assegna comunque il numero di protocollo e registra l'evento sia sul log applicativo/sistema (Speed-log.txt e SystemOut.log) sia sulla tabella interna Oracle D_EVENTI.

Il malfunzionamento viene segnalato all'utente finale del sistema mediante un opportuno diagnostico e l'operazione di archiviazione potrà essere ripetuta al ripristino del servizio del Sistema Documentale (opportunamente monitorato attraverso delle sonde di sistema che attivano i diversi scenari operativi per il ripristino funzionale).

Le decodifiche degli errori vengono mappate mediante l'apposita tabella Oracle D_ERRORI e possono essere raggruppati in questi macrogruppi:

- Errore di accesso servizio Documentale
- Errore durante la verifica del servizio Documentale
- Errore inizializzazione PDFService
- Runtime all'interno dell'applicativo Protocollo
- Errore nel trattamento dei messaggi di posta
- Il processo di acquisizione di un documento può diversificarsi nelle seguenti tipologie:
    - Acquisizione da scanner
    - Acquisizione da file system locale
    - Acquisizione da messaggio di posta
    - Acquisizione da un processo di scansione massiva
    - Acquisizione attraverso servizi web

La conversione di una tipologia di documento in formato PDF è esterna all'applicativo e resa da un servizio web.

E' importante sottolineare, che a scopo di prevenire situazioni di errore nella componente on line della soluzione, sono state implementate sul sistema un meccanismo di sonde automatiche che ripercorrono i flussi utente maggiormente utilizzati. Nel caso di errore nella navigazione simulata, viene inviata una mail di allarme ad una lista di destinatari, costituita da personale tecnico specializzato. Questo al fine di intervenire in maniera tempestiva al verificarsi di malfunzionamenti.

Relativamente ai malfunzionamenti relativi al colloquio trai processi asincroni e i sistemi di PEC e PEL, gli stessi vengono tracciati nei log applicativi presenti sui server. Esistono inoltre, per questi

servizi asincroni di colloqui con la PEC e PEL, dei processi di verifica schedulati periodicamente durante il giorno, che interrogando le banche dati rilevano le eventuali anomalie o blocchi, e provvedono ad inviare delle notifiche ad una lista di destinatari, specializzati nel trattamento di questi problemi.

Numerator Layer
Questa nuova componente, caratterizzata dal requisito di avere elevati livelli di performaces non traccia log delle transazioni.
Possono essere attivate all'occorrenza, per valutare eventuali fenomeni opportune trace, ma per periodi molto brevi, al fine di non incidere sulle prestazioni.

39. Sicurezza dell'infrastruttura

-SEGMENTAZIONE DELLE RETI

L'intera infrastruttura risiede su rete interna campus (ad eccezione di un componente, in DMZ per l'interfacciamento con le CRL su internet). E' comunque stata prevista una suddivisione dei nodi di back-end e front-end in base ai loro ruoli.
Approfondendo in maggiore dettaglio i presidi di sicurezza presenti sulle reti dell'architettura, si evidenzia quanto segue:

- Le reti DMZ esposte su internet, in particolare quella bilanciata relativa ai server di front-end, la rete dei server CRL di verifica firma digitale, nonché la DMZ separata contenente i front-end ed i relay server della PEC, sono tutte protette, oltre che dai Firewall perimetrali, anche da sonde per l'Intrusion Prevention (IPS inline, che effettuano il drop dei pacchetti in caso di rilevazione di attacco).
- La rete DMZ che ospita i nodi di verifica della firma digitale e quella dedicata ai front-end di PEC sono ulteriormente separate dalla rete interna per mezzo di Firewall, in modo da consentire il traffico solo tra host autorizzati nell'ambito dell'architettura.
- Le reti separate sono gestite da bilanciatori CSS che espongono degli indirizzi virtuali dei cluster di server fisici, in modo da garantire l'alta affidabilità degli apparati

-CONFIDENZIALITÀ DEI DATI

Trattandosi di comunicazioni su reti interne, segmentate come sopra descritto, lo scambio di pacchetti avviene in chiaro senza crittografia, sia per permettere una analisi di tali pacchetti alle sonde di sicurezza sulla rete, sia per motivi di compatibilità col prodotto "Speed Engine" integrato nell'infrastruttura.
Su tutti i sistemi della infrastruttura l'accesso di utenze privilegiate è mediato dal prodotto CyberArk.
Sugli application server WebSphere di back end è poi attiva l'autenticazione integrata tramite LTPA-token, per la gestione delle credenziali.

L'autenticazione si basa su Active Directory e sull'integrazione WebSphere con AD e Kerberos per la realizzazione del meccanismo di SSO tra le postazioni di lavoro e la Applicazioni Web.

L'utente può accedere al repository documentale attraverso un meccanismo di propagazione d'identità (SSO) basato su RSA Access Managersolo dopo essersi autenticato sulla Applicazione di front-end.
Relativamente al back end Documentum, l'attuale configurazione del repository a servizio del cliente prevede che utenti e gruppi siano quotidianamente sincronizzati con i Directory Server (CAU) in modo che la profilazione utente venga gestita all'esterno della piattaforma documentale. Quindi gli utenti che possono accedere ad uno specifico repository Documentum sono censiti anche all'interno del repository documentale stesso.
Se gli utenti finali accedessero alla piattaforma con credenziali, Documentum verificherebbe su CAU la password; poiché l'accesso è fatto per propagazione di identità, Documentum verifica il token di SSO.
Per alcuni flussi, è previsto l'uso di una utenza Documentum di servizio: l'utenza di servizio è una utenza interna a Documentum, accede con credenziali, e la sua password è verificata su repository.
L'applicazione accede alla piattaforma documentale tramite le Java API DFC (Documentum Foundation Class): le DFC prevedono un metodo per criptare una password, non pubblicano alcun metodo DFC per decifrarla, prima di inviarla alla piattaforma.
L'uso degli oggetti documentali (contenuti e metadati) è controllato da meccanismi di ACL, interni alla piattaforma Documentum, associati puntualmente ad ogni oggetto.

-BILANCIAMENTO E RIDONDANZA

Di seguito vengono elencati gli elementi peculiari dell'infrastruttura e le modalità con cui sono stati realizzati bilanciamento e ridondanza:

- una farm di Web Server deputati all'accoglienza, su cui è installato IBM HTTP Server; i web server sono attestati su rete bilanciata per garantire continuità del servizio e bilanciamento;
  lo strato applicativo è ospitato su una batteria di server su cui è installato IBM WebSphere Application Server Network Deployment 8.5.5.5 in modalità clustering a garanzia di bilanciamento e alta affidabilità; l'alta affidabilità dei Web Server e Application Server è garantita dalla piattaforma VMware
- il servizio "PDF Converter", erogato attraverso Web Server IIS, è offerto da una coppia di server Windows installati su rete bilanciata a garanzia sia di continuità del servizio che di bilanciamento del carico elaborativo
- allo scopo di realizzare una architettura bilanciata ed in alta affidabilità, la piattaforma documentale è stata distribuita su quattro server bi-processori quadcore a 64 bit:
  -una coppia di server offre il servizio del Content Server ridondato, contattato direttamente dalla Applicazione: in tal caso il bilanciamento è implementato mediante la componente client della piattaforma documentale stessa, richiamata dall'Applicazione
  -la seconda coppia di server ospita i servizi di Searching e di Indexing anch'essi ridondati e configurati in alta affidabilità; in tal caso il bilanciamento è stato realizzato attestando i due server su rete bilanciata.
- relativamente alla componente DB Server sono stati realizzati due ambienti: uno ospita il DB applicativo e l'altro il DB del prodotto documentale; per i dettagli si rimanda al paragrafo "software e tecnologie adottati per garantire la disponibilità e l'integrità dei dati".
- relativamente alle aree di Storage, sia per i dati del DB che per la memorizzazione del documento, si rimanda al paragrafo "dettagli tecnologici sottosistemi disco per garantire la disponibilità e l'integrità dei dati".

-INTEGRITÀ DEI DATI

Software e tecnologie adottati

Come si accennava in precedenza, in merito alla componente DB sono stati realizzati due ambienti: uno ospita il DB applicativo e l'altro il DB del prodotto documentale.

Le tecnologie utilizzate per garantire la massima disponibilità e sicurezza nella gestione dei dati sono al massimo livello di quelle attualmente disponibili sul mercato.

In particolare il database applicativo è stato ospitato su un sistema Exadata X8-2 Full Rack.

Sia Oracle Exadata Database Machine che Oracle SPARC SuperCluster aderiscono ai massimi standard di:

- affidabilità: lato hardware l'Exadata Database Machine non ha "single point of failure"; tutte le componenti hardware (comprese le connessioni alla rete elettrica, gli switch di rete interni e quelli che la collegano al mondo esterno) sono ridondate, pertanto il sistema è in grado di offrire una elevato livello di affidabilità,
- disponibilità: il software Oracle ed in particolare le sue componenti Real Application Cluster (RAC) e Automatic Storage Manager (ASM) garantiscono la massima disponibilità delle basi di dati ospitate a bordo della Exadata Database Machine, garantendo che eventuali malfunzionamenti hardware o software non impattino sulle attività degli utenti finali,
- scalabilità: la soluzione è perfettamente scalabile sia lato sottosistema di gestione di Oracle Database (nuovi nodi DB server possono essere aggiunti dinamicamente alla soluzione) sia lato storage (nuovi Exadata Storage Server possono essere aggiunti alla configurazione iniziale) senza interruzioni di servizio e con presa in carico automatica da parte delle componenti software del sistema delle nuove risorse disponibili.

La componente innovativa nell'architettura di un sistema Exadata, rispetto ad un ambiente Oracle convenzionale è costituita dall'Exadata Storage Server Software che, eseguito a livello delle singole unità di storage, svolge un insieme di funzioni che consentono di ottenere prestazioni elevate in qualunque contesto applicativo:

1. Smart Scan, funzionalità che consente la drastica riduzione dei dati scambiati da storage a database server e lo spostamento di logiche di "ricerca" dei dati sugli storage server;
2. gestione di Storage Indexes, funzionalità che consente la riduzione delle richieste di I/O verso i dischi;
3. Hibryd Columnar Compression, funzionalità che consente di ridurre lo spazio fisico richiesto per la memorizzazione dei dati sullo storage e, contemporaneamente, di ridurne i tempi di recupero (più operazioni di I/O su dati non compressi possono essere sostituite da una sola operazione di I/O su dati compressi) ed il trasporto sui canali di interconnessione fra i sottosistemi storage e database server;
4. gestione delle Flash Memory: la gestione di queste memorie non volatili ad altissima velocità (a livello locale degli storage server) come cache "intelligenti" (ad evitare fenomeni, ad esempio, di cache pollution) fa sì che i singoli storage server possano rispondere in modo sempre più veloce alle richieste di I/O ricevute dai database server.

Per quanto riguarda Exadata, la protezione dai failure di tipo storage è data dal volume manager utilizzato all'interno di Exadata (Oracle Automatic Storage Management - ASM) che utilizza, nell'implementazione Sogei, la policy di mirroring NORMAL (a due vie) o superiore.

Per quanto riguarda il database del sistema documentale risiede su un cluster a 2 nodi, ospitati su due sistemi IBM 9119. Le 2 LPAR (Logical Partitions) sono dotate di sistema operativo IBM AIX 6.1

,software di cluster IBM HACMP e un Oracle per ospitare la banca dati del documentale sistemi IBM 9119 Power 595 ospitano ciascuno 64 core, con processore IBM POWER6 ad altissima frequenza e configurazioni SMP (Symmetric Multi-Processing). Il Power 595 è in grado di scalare rapidamente e facilmente grazie alla funzioni di virtualizzazione avanzate PowerVM, alla tecnologia EnergyScale e alle opzioni di CoD (Capacity on Demand).
Il sistema operativo utilizzato è IBM AIX 6.1 64 bit, basato sulle funzioni di virtualizzazione e sulla tecnologia POWER6, offre prestazioni superiori alla precedente versione AIX 5L, garantisce un maggiore utilizzo ed efficienza del sistema. AIX 6.1 è un sistema operativo UNIX basato su open standard compatibile con Single UNIX Specification Version 3 di Open Group.
IBM General Parallel File System (GPFS) Multiplatform, consente l'accesso simultaneo di applicazioni parallele a una serie di file (o anche ad un singolo file) dai nodi con file system GPFS, fornendo un livello elevato di controllo su tutte le attività dei file system.
IBM High Availability Cluster Multiprocessing per AIX (HACMP™) consente di ottenere la business continuity necessaria per garantire il ripristino dei servizi in caso di fault di un sistema del cluster. L' HACMP fornisce servizi di alta disponibilità, monitorando le risorse condivise ed i servizi ospitati in cluster, nel nostro caso il DB oracle del documentale.
Tutte le componenti hardware dei server sono ridondate per garantire la massima disponibilità (dischi, alimentazione, schede di Lan, schede storage); inoltre i sistemi, tramite la tecnologia Power, permettono la sostituzione a caldo di memoria e cpu, con le componenti disponibili nei server.

Dettagli tecnologici sottosistemi DISCO
Mentre per il DB applicativo lo storage è già integrato nel sistema EXADATA per la parte documentale l'architettura individuata è articolata come segue.
Storage Database:

- Al primo livello i device sono stati definiti su uno degli storage Hitachi 9990V presenti in Sogei. Si tratta di uno storage di classe enteprise che nella specifica configurazione utilizzata usufruisce di dischi di tecnologia FC da 146 GB a 15 krpm, con livello di protezione RAID1, nonché di 256 GB di cache condivisa in grado d'assicurare elevatissimi livelli di throughput.
- Lo storage ha un'architettura completamente ridondata per quanto riguarda l'alimentazione elettrica, i canali di comunicazione interni ed esterni così come per la cache, ed è dotato di dischi di spare che intervengono ogniqualvolta un disco interno accusi un fault così d'assicurare sempre e comunque il livello di RAID impostato. I device sono stati quindi esportati sul virtualizzatore storage Hitachi 9985V che ha caratteristiche equiparabili all'Hitachi 9990V così da offrire performance comparabili a quelle dello storage base.
- Su quest'ultimo sono state definite le ACL riguardanti l'acceso dei server. La ridondanza è assicurata anche per quanto riguarda i collegamenti in fibra sugli switch della SAN.

Storage Memorizzazione Documenti:

- lo storage utilizzato è di tipo NAS. Nello specifico il modello utilizzato e lo EMC2 VNX7500 che espone i filesystem utilizzando il protocollo NFS. Sui filesystem oggetto di condivisione sono state definite le ACL in modo tale che l'accesso sia consentito solamente agli host abilitati. Per garantire un elevato grado di protezione del dato le share sono oggetto di due repliche entrambe in modalità asincrona, una locale ed una remota. La prima, quella locale, prevede la copia del dato su un gateway modello EMC2 VG8 che ha i dischi definiti su due storage modello EMC2 CX4. La seconda copia è stata configurata su uno storage, stesso modello del primario lo EMC2 VNX7500, installato presso il sito di disaster recovery.

- La ridondanza delle componenti interne di entrambi gli storage garantiscono livelli di sicurezza elevati.

Policy utilizzate dal DBMS: criteri di protezione del DB, controllo accessi

Gli ambienti sono predisposti per l'adeguamento a regole di autenticazione/autorizzazione considerate requisito minimo, anche in termini di rapporto costo/beneficio, per innalzare il livello di sicurezza degli ambienti.

Tipicamente i problemi in ambito sicurezza derivano dall'utilizzo di una login generica per l'accesso ai dati; per innalzare il livello di sicurezza si rende dunque necessario:

- disabilitare la possibilità di login mediante lo schema possessore degli oggetti del database relativi all'applicazione;
- utilizzare login individuali (sottoposte ad audit) per il personale Sogei; gli amministratori di sistema possono accedere alle base di dati in due modalità:
- attraverso le utenze anonime di sistema: in questo caso vengono utilizzate delle credenziali presenti su un repository CyberArk. Le credenziali presenti su questo repository sono sottoposte a meccanismi di password policy. L'utilizzo di queste credenziali di sistema da parte di un amministratore viene tracciata attraverso il prodotto Secure Log. Questi tracciamenti sono mantenuti in linea per 6 mesi e successivamente trasferiti su memorie di massa meno performanti
- attraverso la propria utenza personale.
- Indipendentemente dal tipo di accesso effettuato da una figura umana (non da un sistema) i comandi eseguiti sul DBMS, sono tutti tracciati e tenuti in linea su una banca dati per 6 mesi. Trascorso questo tempo gli stessi vengono trasferiti su memorie di massa meno performanti.
- utilizzare per le login generiche tipiche dei pool di connessione degli application server e dei batch, delle login distinte dallo schema possessore delle tabelle; l'accesso al database da parte di tali login viene limitato in base all'indirizzo IP del server di back-end di provenienza.

Tali login vengono profilate in base al criterio del privilegio minimo, cioè con le grant strettamente necessarie per il corretto funzionamento dell'applicazione.

Oltre all'autenticazione, particolare attenzione è posta verso il meccanismo di autorizzazione che include fondamentalmente due processi:

1) il primo introduce limiti sulle risorse del sistema (CPU, memoria, sessioni, idle time, …) sugli accessi e sulle azioni degli utenti connessi al sistema;

2) il secondo consiste nel limitare agli utenti l'accesso, la modifica ed il trattamento dei dati.

Per quanto riguarda il primo punto, cioè l'uso delle risorse di sistema, è stato introdotto l'uso dello strumento Resource manager di Oracle, mediante il quale è possibile:

- garantire ad alcuni utenti una quantità minima di risorse elaborative a prescindere dal carico del sistema e dal numero di utenti connessi;
- distribuire le risorse di elaborazione disponibili, allocando differenti percentuali di CPU a differenti utenti ed applicazioni;
- limitare il grado di parallelismo che ciascun utente può utilizzare.

A livello generale si è scelto di definire, per quanto riguarda l'utilizzo della CPU, una politica di priorità gerarchica tra i vari utenti, tale che le risorse non utilizzate dagli utenti di un livello superiore vengono messe a disposizione degli utenti a priorità inferiore.

La priorità è assegnata in maniera decrescente ai seguenti profili:

- WEB utilizzato per il core-business dell'applicazione;
- OLTP utilizzato per le utenza Sogei e per i rami non critici dell'applicazione;
- BATCH utilizzato per le applicazioni batch.

La scelta di privilegiare il profilo web deriva dal fatto che in generale è quello su cui si definiscono i livelli di servizio.
In conclusione, per quanto riguarda l'utilizzo del Resource manager, viene chiesto al personale dei progetti interessati di mappare le varie login generiche ai tre profili definiti.
Per quanto riguarda il punto 2) al fine di limitare il rischio di abuso di privilegi, vengono assegnati ruoli alle varie login (quelle dei pool di connessione degli application server, quelle dei batch server e quelle del personale SOGEI) in funzione dei differenti profili operativi, basandosi sul criterio del privilegio minimo.
In particolare:

- non potrà essere concesso nessun privilegio di tipo ANY (ad esempio alter any table)
- l'uso del package UTL_FILE, sempre per motivi di sicurezza, viene concesso solo in casi eccezionali e comunque concordato col dba di riferimento
- sono disabilitati i package UTL_SMTP, UTL_TCP, UTL_HTTP
- non viene consentita l'esecuzione di External Procedure (routine C, COBOL, … richiamabili da PL/SQL); la logica applicativa viene incapsulata il più possibile in package

-BACKUP SISTEMI E DATI

Per la salvaguardia dei dati di un'infrastruttura così complessa, viene utilizzata la soluzione di backup, adottata come standard Sogei, basata su software Symantec Netbackup. Essa è implementata mediante un insieme di server (media server) che operano, condividendola, su una libreria Sun Stk SL8500 in grado di ospitare fino a 7.000 tape. In affiancamento alla libreria fisica vi è una disk library con funzione di VTL (virtual Tape Library) che può operare in modalità deduplicata.

Database Applicativo

Anche se Oracle e gli Exadata Storage Cell incorporano numerose funzionalità dedicate alla protezione dalla corruzione dei dati memorizzati, tali funzionalità devono comunque essere affiancate da una soluzione di backup che assicuri la possibilità di ripristinare i dati in caso di corruzioni logiche anche su intervalli temporali estesi.
Oracle Recovery Manager (RMAN) fornisce l'infrastruttura nativa di backup e restore di Oracle Database abilitando una protezione dei dati ottimizzata per l'Exadata Database Machine:

1. Il Backup, Restore e operazioni di ripristino sono eseguite usando i comandi standard di RMAN
2. RMAN può parallelizzare le operazioni di backup su tutte i nodi database e le Exadata Storage Cell. Questa ottimizzazione permette di raggiungere valori elevati di prestazioni in funzione del backup.
3. La tracciatura dei blocchi modificati permette di eseguire backup incrementali veloci ed efficienti. Solo le aree del database che sono modificate dall'ultimo backup incrementale vengono lette dal disco.

In base al valore di RTO ottenibile sono possibili tre principali scenari di Backup.

Soluzione di Backup	RTO [base temporale]
DataGuard su altro Exadata Database Machine/SPARC Supercluster	secondi
Disk-to-Disk	1 ora per 10 TB
Disk-to-Tape	5 ore per 10 TB

La prima soluzione permette di ottenere i valori più bassi di RTO ed RPO e si adatta a contesti mission-critical. Questa soluzione utilizzando le funzionalità di replica remota Data Guard di Oracle Database è più simile ad una Business Continuity o ad un Disaster Recovery che ad una vera soluzione di Backup e Restore.
Per il progetto in questione le due soluzioni di backup su disco e su tape (D2D e D2T) sono state implementate contemporaneamente in modo da assicurare un efficiente tempo di ripristino (soluzione disk-to-disk) ed una elevata retention (soluzione disk-to-tape) in una unica architettura detta disk-to-disk-to-tape: D2D2T.
L'implementazione adottata per la soluzione D2D2T è basata sulle funzionalità native di RMAN; i backup vengono prima eseguiti su un appliance esterno (Oracle ZFS Storage Appliance). Appena prodotti i backupset su disco, rman legge attraverso il canale di comunicazione ad alta velocità presente all'interno dell'Exadata (rete infiniband) e li invia sempre via infiniband al backup server che li copia su nastro.
Di seguito viene presentato il tipico disegno architetturale di questa soluzione.

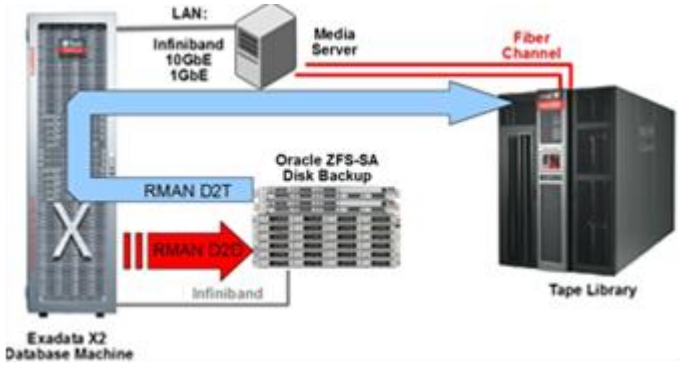

Figura 7: Soluzione D2D2T con RMAN

Database documentale
La stessa infrastruttura utilizzata dalla parte dei DB viene utilizzata per il salvataggio della parte NAS. In questo caso però Netbackup ha la possibilità di interfacciare direttamente i gateway NAS per fare il backup dei dati attraverso un protocollo denominato NDMP.
Documenti contenenti Dati Sensibili
I documenti con dati sensibili sono memorizzati nel sistema sottoforma di documento crittografato. La crittografia viene temporaneamente rimossa dallo strato applicativo quando a consultare il documento è un utente che gode dei privilegi per poterlo fare ed è stato preventivamente autorizzato. È da tener presente che il documento archiviato rimane sempre crittografato, mentre l'utente autorizzato utilizza una versione in chiaro temporaneamente e solo nell'ambito dello scope funzionale.

-BUSINESS CONTINUITY E DISASTER RECOVERY

Attualmente non sono state espresse indicazioni per l'attivazione del servizio secondo quanto previsto nel CSQ.

-MONITORAGGIO DEL SERVIZIO

Il servizio è sottoposto a monitoraggio di funzionamento secondo i termini e gli orari definiti nei requisiti del servizio stesso.

40. Modalità richiesta informazione dati

Sogei riceve dall'Autorità Giudiziaria e dai clienti istituzionali le richieste riguardanti il reperimento delle operazioni registrate negli archivi del Sistema Informativo della Fiscalità (SIF) aventi carattere riservato e considerate come Dati Tutelati.
Tali richieste, protocollate nell'apposito Registro Ufficio Sicurezza dell'applicazione Protocollo, riguardano in particolare:

- l'estrazione puntuale o massiva di informazioni su cittadini registrati nelle banche dati del SIF;
- il tracciamento delle operazioni di accesso e utilizzo dei servizi informatici effettuati dagli utenti del SIF e registrate negli archivi di log;
- l'estrazione di informazioni di tracciamento di posta elettronica e navigazione Internet.

Sulla base della tipologia, le richieste sono assegnate alla struttura aziendale competente che provvede a ricercare le operazioni richieste, eventualmente coadiuvata dal supporto sistemistico dell'esercizio, e fornire le informazioni relative all'esito della ricerca.

Allegato 1 - Descrizione della *AOO*

DENOMINAZIONE DELLA *AOO*	UFFICIO DI SEGRETERIA DEL CONSIGLIO DI PRESIDENZA DELLA GIUSTIZIA TRIBUTARIA
CODICE IDENTIFICATIVO	DFCPGT
INDIRIZZO DELLA SEDE DELLE *AOO*	VIA SOLFERINO, 1 5 00184 ROMA
CASELLA DI POSTA ELETTRONICA CERTIFICATA	ufficiosegreteriaCPGT@pce.finanze.it
DATA DI ISTITUZIONE DELLA *AOO*	5 NOVEMBRE 2015 Decreto DGF Prot. n. 14/2015 del 5-11-2015 - DF.DSI.Registro Repertorio
RESPONSABILI DELLA GESTIONE DOCUMENTALE DELLE *AOO*	- IL DIRIGENTE *PRO TEMPORE* INCARICATO DELLA DIREZIONE DELL'UFFICIO DI SEGRETERIA DEL CONSIGLIO DI PRESIDENZA DELLA GIUSTIZIA TRIBUTARIA
AMMINISTRATORI DELL'*AOO*	TRAVAGLINI ANTONELLA MARENGA STEFANO

Prot. n. 14/2015 DF.DSI. Registro Repertorio

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLE FINANZE

IL DIRETTORE GENERALE DELLE FINANZE

VISTO il decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 recante il "Testo Unico delle disposizioni legislative e regolamenti in materia di documentazione amministrativa" (di seguito "testo unico");

VISTO il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il "Codice dell'Amministrazione Digitale";

VISTO il decreto del Presidente del Consiglio dei Ministri del 27 febbraio 2013, n. 67, recante il "Regolamento di organizzazione del Ministero dell'economia e delle finanze";

VISTO il decreto ministeriale 17 luglio 2014, concernente l'individuazione e le attribuzioni degli uffici di livello dirigenziale non generale dei Dipartimenti del Ministero dell'Economia e delle Finanze, pubblicato nel Supplemento Ordinario n. 75 alla Gazzetta Ufficiale – serie generale – del 15 settembre 2014, n. 214;

VISTO il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-*bis*, 41, 47, 57*bis* e 71 del Codice dell'Amministrazione digitale, pubblicato nel Supplemento Ordinario n. 20 alla Gazzetta Ufficiale – serie generale – 12 marzo 2014, n. 59;

VISTO in particolare l'art. 3 del sopra citato DPCM 3 dicembre 2013 che stabilisce l'obbligo

per le pubbliche amministrazioni di individuare le aree organizzative omogenee (*AOO*) e i relativi uffici di riferimento ai sensi dell'art. 50 del testo unico, e di nominare in ciascuna *AOO* il responsabile della gestione documentale;

VISTO in particolare l'art. 4, comma 1, del citato DPCM 3 dicembre 2013, che definisce i compiti del responsabile della gestione documentale;

VISTO il decreto direttoriale prot. 2435 del 27 novembre 2009 con il quale sono state istituite le Aree Organizzative Omogenee (*AOO)* per la gestione del Protocollo Informatico;

RITENUTO di dover procedere alla ricognizione delle *AOO* del Dipartimento delle finanze e alla conseguente designazione dei responsabili della gestione documentale;

CONSIDERATO di dover in parte modificare il citato decreto direttoriale prot. n. 2435 del 27 novembre 2009 per renderlo coerente con il mutato assetto organizzativo introdotto dal DPCM 27 febbraio 2013, n. 67;

DECRETA

Art. 1

A parziale modifica del decreto direttoriale prot. n. 2435 del 27 novembre 2009, le Aree Organizzative Omogenee (*AOO*) del Dipartimento delle Finanze per la gestione documentale e il protocollo informatico, sono le seguenti:

6 *AOO* corrispondenti alle Direzioni centrali del Dipartimento delle finanze;

1 *AOO* corrispondente agli Uffici assegnati alle dirette dipendenze del Direttore Generale del Dipartimento;

103 *AOO* corrispondenti delle Commissioni Tributarie Provinciali, comprese le Commissioni tributarie di 1° grado di Bolzano e Trento

21 *AOO* corrispondenti agli Uffici di segreteria delle Commissioni Tributarie Regionali, comprese le Commissioni tributarie di 2° grado di Bolzano e Trento;

1 *AOO* corrispondente all'Ufficio di segreteria del Consiglio di Presidenza della Giustizia Tributaria.

Art. 2

Sono nominati responsabili della gestione documentale, di cui all' art. 3, comma 1, del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013:

- i dirigenti *pro tempore* incaricati della direzione dell'Ufficio I in ciascuna Direzione centrale del Dipartimento;
- il dirigente *pro tempore* incaricato della direzione dell'Ufficio II alle dirette dipendenze del Direttore generale delle finanze;
- i direttori *pro tempore* degli uffici di segreteria delle Commissioni provinciali, regionali e del Consiglio di Presidenza della Giustizia Tributaria.

Roma, 5 novembre 2015

Fabrizia Lapecorella
[*firmato digitalmente*]

Allegato 3 –
Decreto di nomina del Coordinatore della gestione documentale

Prot. n. 15/2015 DF.DSI. Registro Repertorio

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLE FINANZE

IL DIRETTORE GENERALE DELLE FINANZE

VISTO il decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 recante il "Testo Unico delle disposizioni legislative e regolamenti in materia di documentazione amministrativa";

VISTO il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il "Codice dell'Amministrazione Digitale";

VISTO il decreto del Presidente del Consiglio dei Ministri del 27 febbraio 2013, n. 67, recante il "Regolamento di organizzazione del Ministero dell'economia e delle finanze";

VISTO il decreto ministeriale 17 luglio 2014, concernente l'individuazione e le attribuzioni degli uffici di livello dirigenziale non generale dei Dipartimenti del Ministero dell'Economia e delle Finanze, pubblicato nel Supplemento Ordinario n. 75 alla Gazzetta Ufficiale – serie generale – del 15 settembre 2014, n. 214;

VISTO il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "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-*bis* e 71, comma 1, del Codice dell'Amministrazione digitale, pubblicato nel Supplemento Ordinario n. 20 alla Gazzetta Ufficiale – serie generale – 12 marzo 2014, n. 59;

VISTO il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-*bis*, 41, 47, 57*bis* e 71 del Codice dell'Amministrazione digitale, pubblicato nel Supplemento Ordinario n. 20 alla Gazzetta Ufficiale – serie generale – 12 marzo 2014, n. 59;

VISTO in particolare l'art. 3, comma 1, lett. *c)* del citato DPCM 3 dicembre 2013, che prevede, nell'ambito delle amministrazioni con più aree organizzative omogenee (*AOO*), la nomina del coordinatore della gestione documentale e del suo vicario per i casi di vacanza, assenza o impedimento del primo;

VISTO il decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-*bis*, 23-ter, 40, 41 e 71, comma 1, del Codice dell'Amministrazione digitale, pubblicato nella Gazzetta Ufficiale – serie generale – 12 gennaio 2015, n. 8;

RITENUTO di dover procedere alla designazione del coordinatore della gestione documentale e del suo vicario, relativamente ai documenti amministrativi informatici prodotti dalle strutture centrali e dalle Commissioni tributarie del Dipartimento delle Finanze;

DECRETA

Art. 1

La dott.ssa Russo Franca, dirigente di seconda fascia del Ruolo dei dirigenti del Ministero dell'Economia e delle Finanze, è nominata Coordinatore della gestione documentale relativamente ai documenti amministrativi informatici gestiti dalle strutture centrali e dalle Commissioni tributarie del Dipartimento delle Finanze.

Art. 2

Il dott. Antonioli Luciano, appartenente all'Area 3, fascia retributiva 5, è nominato vicario del Coordinatore della gestione documentale di cui all'art. 1.

Art. 3

Il Coordinatore della gestione documentale e il suo vicario svolgono i compiti loro affidati dalle citate Regole tecniche sul sistema di conservazione (DPCM 3 dicembre 2013), sul protocollo informatico (DPCM 3 dicembre 2013) e sulla formazione e gestione dei documenti informatici (DPCM 13 novembre 2014).

In modo peculiare, ai sensi dell'art. 4, comma 2 delle citate Regole tecniche sul protocollo informatico, hanno il compito di definire e assicurare criteri uniformi di trattamento del documento amministrativo informatico e, in particolare, di classificazione e archiviazione, nonché di comunicazione interna tra le *AOO* del Dipartimento delle finanze.

Roma, 5 novembre 2015

Fabrizia Lapecorella

[*firmato digitalmente*]

CPGT – UFFICIO DI SEGRETERIA DEL CONSIGLIO DI PRESIDENZA DELLA GIUSTIZIA TRIBUTARIA

- AA Supporto alla stipula ed alla gestione delle convenzioni con le Agenzie *

- 01 SEGRETERIA GENERALE *
  - 01 SEGRETERIA DELLA PRESIDENZA *
    - 01 Attività di Segreteria *
    - 02 Attività Consiliari *
    - 03 Rapporti esterni *
  - 02 SEGRETERIA AMMINISTRATIVA *
    - 01 Gestione del personale *
      - 01 Normativa, circolari e direttive *
      - 02 Fascicolo personale *
      - 03 Gestione economica *
      - 04 Relazioni sindacali *
      - 05 Formazione del personale *
    - 02 Gestione risorse finanziarie *
      - 01 Autorizzazioni ai pagamenti (spese varie funzionamento ufficio) *
      - 02 Rimborsi personale per missioni *
    - 03 RAPPORTI CON ALTRE P.A. *
  - 03 SEGRETERIA COORD. ATTIVITA' INFORMATICHE *
    - 01 Rapporti esterni p.a. *
    - 02 Rapporti esterni privati *
  - 04 RAGIONERIA *
    - 01 CONTABILITA' *
      - 01 Fatture *
      - 02 Rapporti esterni *
      - 03 Rimborsi esterni *
      - 04 Rimborsi interni (Consiglieri e personale CPGT) *
      - 05 Personale *
      - 06 gestione del bilancio CPGT *
    - 02 ECONOMATO *

- 02 CONSIGLIO *
  - 01 GESTIONE DEI GIUDICI TRIBUTARI *
    - 01 Gestione concorsi *
    - 02 Status dei giudici tributari *
    - 03 Incompatibilità *
    - 04 Compensi ai giudici *
    - 05 Disciplina *
    - 06 Contenzioso *
    - 07 Formazione/aggiornamento giudici tributari *
    - 08 ASSENZE GIUDICI A VARIO TITOLO *
  - 02 STUDI E DOCUMENTAZIONE *
    - 01 Pareri e proposte
    - 02 Normativa sulla G.T.
    - 03 Pubblicazioni del Consiglio
    - 04 Biblioteca Consiglio
    - 05 Rassegna Stampa
  - 03 RAPPORTI CON LA STAMPA
  - 04 RAPPORTI CON IL PARLAMENTO *
    - 01 Interrogazioni parlamentari *
    - 02 Varie *
  - 05 SVILUPPO/AGGIORNAMENTO INFORMATICA PER GIUDICI TRIBUTARI *
  - CPO COMITATO PARI OPPORTUNITA' PER I MAGISTRATI TRIBUTARI
    - COMUNICAZIONI COMUNICAZIONI
    - CONVOCAZIONI CONVOCAZIONI

- 03 SERVIZIO per la tenuta del protocollo *
  - 01 Fascoli generali dei Giudici tributari

Allegato 5 - Richiesta di annullamento di protocollazione

Al Responsabile della gestione documentale
dell'Ufficio di Segreteria del CPGT

SEDE

Prot. n. ___ del _____

OGGETTO: Richiesta di annullamento di protocollazione

Il/la sottoscritto/a _____ funzionario (ovvero Sostituto del Dirigente) dell'Ufficio ___ di questa Segreteria chiede l'annullamento del protocollo n. _____ del _____ per i seguenti motivi:

_____

_____

_____

Li, _____

FIRMA
.....

Autorizzazione all'annullamento di protocollazione

AUTORIZZAZIONE n. ___/__ __ 201__

Prot._____ del _____

Vista la richiesta motivata presentata da __*(nome) (cognome) (qualifica)*__dell'Ufficio ____ in data _____ prot. n. _____si autorizza l'annullamento del protocollo n. _____ del _____.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro di protocollo della Segreteria, così come la data, l'ora e l'autore dell'annullamento e gli estremi della presente autorizzazione all'annullamento.

Li, _____ Il Responsabile della gestione documentale

……

Allegato 6 –Schema incaricati trattamento documenti riservati

Ministero
dell'Economia e delle Finanze

Consiglio di Presidenza della Giustizia Tributaria
IL SEGRETARIO GENERALE

Al Signor _____

Al Signor _____

e, p.c.

All'Amministratore di AOO

Oggetto: individuazione degli operatori incaricati del trattamento dei **dati riservati** nei Servizi Documentali dell'Ufficio di Segreteria del Consiglio di Presidenza della Giustizia Tributaria.

Con riferimento alle necessità funzionali dei Servizi Documentali in oggetto, su proposta del Responsabile della gestione documentale di questo Ufficio di Segreteria, le SS.LL. sono incaricate delle operazioni di registrazione e protocollazione in ingresso ed in uscita dei documenti riservati, nonché, unitamente all'Amministratore di AOO che legge per conoscenza, della loro gestione nelle componenti dei Servizi Documentali.

L'Amministratore di AOO, provvederà ad attribuire alle SS.LL. i permessi applicativi idonei ad effettuare il trattamento dei dati riservati in oggetto.

IL DIRIGENTE

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLE FINANZE

IL DIRETTORE GENERALE DELLE FINANZE

Prot. 10291/2010

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (di seguito "Codice");

VISTO l'articolo 28 del Codice, il quale individua come titolare del trattamento dei dati personali svolto da una pubblica amministrazione "l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza";

VISTO l'art. 29 del Codice, il quale dispone che il titolare del trattamento dei dati designa il responsabile ovvero, ove necessario per esigenze organizzative, i responsabili del trattamento dei dati personali, individuandoli tra soggetti che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

VISTO il decreto n. 10905 del 18 novembre 2005 del Capo del Dipartimento per le politiche fiscali, con il quale vengono designati i Responsabili del trattamento dei dati personali nell'ambito delle strutture del Dipartimento;

VISTO il decreto del Presidente della Repubblica del 30 gennaio 2008, n. 43, recante il regolamento di riorganizzazione del Ministero dell'Economia e delle Finanze;

VISTO il decreto ministeriale 28 gennaio 2009, concernente l'individuazione e le attribuzioni degli uffici di livello dirigenziale non generale dei Dipartimenti del Ministero dell'Economia e delle Finanze, pubblicato nella *Gazzetta Ufficiale* del 1° luglio 2009, S.O. n. 150, in vigore dal 1° settembre 2009;

RITENUTO necessario, alla luce della riorganizzazione delle strutture del Dipartimento delle finanze, aggiornare il citato decreto del Capo del Dipartimento n. 10905 del 18 novembre 2005;

DESIGNA

- i direttori delle Direzioni del Dipartimento e i dirigenti generali assegnati al Dipartimento
- i dirigenti e i reggenti assegnati agli Uffici delle Direzioni del Dipartimento e agli Uffici alle dirette dipendenze del Direttore generale delle finanze

- i direttori e i dirigenti degli uffici di Segreteria delle Commissioni Tributarie Regionali e Provinciali, nonché dell'ufficio di Segreteria della Commissione Tributaria Centrale,
- il direttore e i dirigenti dell'ufficio di Segreteria del Consiglio di Presidenza della Giustizia Tributaria

RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

svolto nell'ambito delle unità organizzative di propria competenza, secondo la definizione dell'art. 4, c. 1, lett. g, del citato Codice. I responsabili del trattamento hanno il dovere di compiere tutto quanto necessario per il rispetto delle disposizioni previste dal Codice.

In particolare dovranno:

- *Garantire* che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;
- *Trattare* in modo lecito e secondo correttezza i dati personali oggetto di trattamento;
- *Garantire* che la raccolta e la registrazione dei dati avvengano per scopi determinati, espliciti, legittimi e che il loro utilizzo in altre operazioni di trattamento avvenga in termini compatibili con tali scopi;
- *Designare* gli incaricati al trattamento dei dati personali tra il personale alle dirette dipendenze, nel rispetto delle disposizioni di cui all'articolo 30 del Codice;
- *Vigilare* sull'applicazione, da parte degli incaricati, delle proprie istruzioni e di quelle impartite da chi esercita le funzioni di titolare;
- *Specificare*, con atto scritto, i profili di autorizzazione degli incaricati individuando a quali dati i medesimi incaricati possono accedere e quali trattamenti (tipi di dati trattati e operazioni eseguibili) sono consentiti;
- *Aggiornare* annualmente l'ambito di trattamento consentito ai singoli incaricati;
- *Assicurare* che i dati siano esatti e, se necessario, aggiornarli;
- *Assicurare* che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- *Conservare* i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- *Custodire e controllare* i dati personali oggetto di trattamento, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità di raccolta;
- *Utilizzare* i dati personali nel rispetto e nei limiti imposti dall'articolo 14 del Codice;

- *Non comunicare e non diffondere* dati personali cancellati o per i quali sia decorso il periodo di tempo di cui all'art. 11 c. 1, per finalità diverse da quelle indicate nella notificazione di cui agli articoli 37 e 38 del Codice;
- *Trattare* i dati sensibili, così come identificati dall'art. 4, c. 1, lett. d, del Codice secondo le modalità di cui all'articolo 20 dello stesso;
- *Limitare* l'accesso ai dati sensibili al solo personale incaricato, adeguatamente istruito sulle modalità di trattamento dei medesimi dati;
- *Assicurare* la conservazione di atti e documenti contenenti dati sensibili e giudiziari in archivi protetti;
- *Disporre* affinché i dati idonei a rilevare lo stato di salute e la vita sessuale siano conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- *Rispettare* le misure di sicurezza predisposte al fine di prevenire accessi e utilizzazioni abusive, non corrette o non conformi alle finalità di raccolta, non solo all'esterno ma anche all'interno dell'Amministrazione;
- *Comunicare* al Titolare le richieste di informazioni o effettuazione dei controlli e accessi da parte del Garante per la protezione dei dati personali;
- *Informare* prontamente il titolare di ogni questione rilevante ai fini del Codice;
- *Rendere* all'interessato l'informativa di cui all'art. 13 del Codice;
- *Rendere* all'interessato le informazioni di cui agli articoli 7 e seguenti del Codice e *provvedere* ai relativi obblighi;
- *Autorizzare* l'accesso ai dati personali in possesso della struttura di appartenenza;
- *Verificare* il trasferimento dei dati personali all'estero ai sensi degli articoli 42, 44 e 45 del Codice;
- *Predisporre* quanto dovuto per le notifiche e le comunicazioni previste dagli articoli 37, 38 e 39 del Codice per la successiva sottoscrizione e l'inoltro all'Autorità del Garante da parte del Titolare;
- *Curare* l'attribuzione dei livelli di autorizzazione per l'accesso a procedure informatizzate, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- *Segnalare* per la disattivazione dei codici identificativi personali, la perdita di qualità d'incaricato dei trattamenti relativamente ai propri collaboratori (per assegnazione a diverso incarico) ed al personale non più in servizio presso l'unità organizzativa (per pensionamento, trasferimento, comando);
- *Osservare* quanto disposto nel documento contenente le "Regole comportamentali sull'utilizzo dei sistemi informatici" adottate all'interno del Dipartimento delle Finanze.

Roma, 3 maggio 2010

Fabrizia Lapecorella

Dipartimento delle finanze

CONSIGLIO DI PRESIDENZA DELLA GIUSTIZIA
TRIBUTARIA
IL SEGRETARIO GENERALE

DISPOSIZIONE DI SERVIZIO

Visto il Decreto legislativo 30 giugno 2003, n. 196: "Codice in materia di protezione dei dati personali", pubblicato nella *Gazzetta ufficiale* del 29 luglio 2003, S.O. n. 174;

Visto l'art. 28 del menzionato Decreto legislativo n. 196/2003, il quale individua come titolare del trattamento dei dati personali svolto da una pubblica amministrazione l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza;

Visto l'art. 29 dello stesso Decreto legislativo n. 196/2003, il quale dispone che il titolare del trattamento dei dati designa facoltativamente il responsabile, individuandolo tra soggetti che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

Visto il comma 1 dell'art. 30 del citato D. Lgs. n. 196/2003, il quale dispone che le operazioni di trattamento dei dati personali possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare del trattamento, o del responsabile del trattamento;

Visto il Decreto direttoriale n. 10291 del 3 maggio 2010 del Direttore generale del Dipartimento delle finanze, con il quale vengono designati quali Responsabili del trattamento, tra gli altri, i Direttori degli uffici di livello dirigenziale generale, e i dirigenti ed i reggenti ad essi assegnati;

VISTO il decreto del Presidente del Consiglio dei Ministri del 27 febbraio 2013, n. 67, recante il "Regolamento di organizzazione del Ministero dell'economia e delle finanze";

VISTO il decreto ministeriale 17 luglio 2014, concernente l'individuazione e le attribuzioni degli uffici di livello dirigenziale non generale dei Dipartimenti del Ministero dell'Economia e delle Finanze, pubblicato nel Supplemento Ordinario n. 75 alla Gazzetta Ufficiale – serie generale – del 15 settembre 2014, n. 214;

Considerato che, ai sensi e per gli effetti delle norme di cui al citato D. Lgs. 196/2003, occorre individuare – tra le unità di personale appartenente all'Ufficio di segreteria del Consiglio di Presidenza della giustizia tributaria – gli incaricati del trattamento dei dati personali;

SI DESIGNANO

quali incaricati del trattamento dei dati personali le seguenti unità di personale:

SI DISPONE

che il personale sopra citato si attenga alle seguenti istruzioni:

- Usare i dati in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati solo per gli scopi inerenti l'attività svolta;
- Verificare, ove possibile, che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti le finalità per cui sono stati raccolti o successivamente trattati;
- Garantire la massima riservatezza dei dati trattati;
- Accedere ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
- Conservare gli atti ed i documenti contenenti i dati e restituirli in archivio al termine delle operazioni affidate.
- Interpellare il dirigente, ovvero, in caso di assenza, il vicario, prima di fornire, all'interessato che ne faccia richiesta, le informazioni relative alla conferma dell'esistenza o meno negli Uffici della Segreteria del Consiglio di Presidenza della Giustizia Tributaria di dati personali che lo riguardano, anche se non ancora registrati.

Il personale incaricato del trattamento dei dati sensibili e giudiziari di cui alle lettere d) ed e) dell'art. 4, comma 1, del D. Lgs. 196/2003, oltre all'adozione delle misure suindicate, avrà cura di:

- Informare il direttore per la formazione di eventuale archiviazione separata da quelli utilizzati per la conservazione di ogni altro dato personale;
- Far annotare la causa della riservatezza nel campo note del protocollo, per consentire l'archiviazione separata;
- Conservare i predetti dati per un periodo non superiore a quello necessario per perseguire le finalità per cui sono stati raccolti;
- Controllare e custodire gli atti e i documenti contenenti i dati sensibili e giudiziari, affidati per lo svolgimento dei compiti assegnati, in maniera che ad essi non possano accedere persone prive di autorizzazione.

Nel caso di allontanamento anche temporaneo dal posto di lavoro, il personale incaricato del trattamento dei dati personali, sensibili e giudiziari, dovrà verificare che non vi sia la possibilità, da parte di terzi, di accedere ai dati per i quali era in corso un trattamento, sia cartaceo che automatizzato.
Nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva e specifica autorizzazione dello scrivente, ovvero, in caso di assenza, del Vicario.
Per quanto non specificato nella presente disposizione di servizio, il personale incaricato del trattamento dei dati personali, sensibili e giudiziari si atterrà alle disposizioni contenute nel D. Lgs. 196/2003, con particolare riferimento agli articoli 11, 18 e 22.

IL DIRETTORE