ASLSassari

LINEE GUIDA PER I RESPONSABILI

ASL 1 di Sassari

La gestione operativa dei sottosistemi informativi aziendali

Queste Linee Guida sono state emesse dal Responsabile della Sicurezza Informatica dell'Azienda USL 1 di Sassari. per definire e uniformare la documentazione delle procedure di Gestione dei Sottosistemi informativi aziendali

Documento	DPS-LGR02/2
Edizione	24/10/2006

Indice del Contenuto

Indice delle figure e Tabelle

Figure

Tabelle

1 Introduzione

1.1 Il contesto di riferimento

Nel corso degli anni, l'informatica si è sviluppata nell'Azienda USL N. 1 di Sassari secondo le priorità di ciascun settore, allo scopo di dotarsi degli strumenti necessari per facilitare l'espletamento di funzioni amministrative o per assolvere a specifici adempimenti.

Attualmente il Sistema Informativo Aziendale è costituito quindi da un'infrastruttura di rete aziendale e da un insieme di sottosistemi informativi settoriali o centrali, che sono dislocati nelle diverse sedi, in locali diversamente attrezzati, e che sono generalmente gestiti dai titolari di ciascun settore.

Si tratta quindi di una situazione disomogenea che è opportuno razionalizzare e uniformare per assicurare un miglior controllo della sicurezza dei trattamenti e dei dati aziendali, con particolare riguardo agli adempimenti richiesti dalla Legge sulla Privacy (DLgs 196/2003 e succ.).

L'Azienda USL 1 di Sassari, dopo aver provveduto nel 2004 agli adempimenti previsti dalla Legge, ha varato nel 2005, con la costituzione del nuovo Settore Sistemi Informativi (SSI), un programma triennale[1] di rinnovamento, razionalizzazione e miglioramento delle proprie infrastrutture informatiche, integrato da un programma di sensibilizzazione e formazione di tutto il personale e degli operatori sanitari in materia di sicurezza dei trattamenti dei dati.

Il Dirigente Responsabile del SSI è stato altresì nominato Responsabile della Sicurezza Informatica, e funge da punto di centrale di raccordo con tutti gli altri Responsabili dei Trattamenti, nominati dal Direttore Generale per assicurare che la gestione e l'utilizzo degli strumenti elettronici sia conformi ai criteri di sicurezza adottati in azienda e alle disposizioni prescritte dalla Legge in materia di Privacy e Sicurezza (D.Lgs 196/2003 e successivi).

1.2 Scopo delle Linee Guida

Queste Linee Guida sono destinate, in primo luogo, a tutti i Responsabili dei Trattamenti, nominati dall'Azienda USL N.1 di Sassari, che hanno anche la responsabilità di gestione di specifici sottosistemi informativi aziendali, siano essi settoriali o centralizzati; in secondo luogo, sono destinate ai fornitori di ICT ai quali è spesso affidata materialmente la manutenzione ed il supporto dei sistemi informatici, affinché essi possano recepire i requisiti dell'Azienda USL N. 1 di Sassari ed adeguare le loro procedure di supporto ed assistenza a quanto specificato in questo documento.

Lo scopo di queste Linee Guida è di fornire un quadro di riferimento per uniformare le modalità di gestione operativa dei sottosistemi informativi aziendali, adottando

[1] Si veda il documento "Sistema Informativo Aziendale - Analisi dello stato delle risorse ICT - Piano triennale di sviluppo 2006-2008 " approvato con Delibera N. 129 del 9 marzo 2006

misure di sicurezza idonee e conformi con quanto richiesto dalla Legge in materia di Privacy e Misure di Sicurezza.

La sicurezza informatica non deve infatti essere intesa solo come protezione da eventi negativi, accidentali o intenzionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi, con particolare riferimento a:

- distruzione o perdita, anche accidentale, dei dati: ossia si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone malintenzionate, mediante processi non autorizzati, o da eventi accidentali;
- accesso non autorizzato ai dati: intendendo in pratica che un determinato dato o informazione deve essere accessibile solo a chi è autorizzato;
- trattamento non consentito o non conforme dei dati: intendendo in pratica che un determinato dato o informazione non debba poter essere trattato in modo non consentito o in modo non conforme alle finalità per il quale il dato o l'informazione era stata raccolta.

In particolare, l'obiettivo primario è di assicurare che la gestione dei sottosistemi informativi aziendali sia adeguatamente e uniformemente documentata, per monitorare centralmente la situazione e pianificare le iniziative di supporto e di miglioramento.

La documentazione richiesta riguarda:

- le caratteristiche fondamentali, le peculiarità e l'ubicazione della piattaforma tecnologica di ciascun sottosistema informativo aziendale;
- l'attribuzione delle competenze e la modalità di gestione di ciascun sottosistema informativo aziendale;
- le misure adottate per prevenire la perdita anche accidentale dei dati critici per l'Azienda;
- la certificazione di conformità di ogni sottosistema informativo aziendale e della sua gestione operativa alle disposizioni del disciplinare tecnico Allegato B del D. Lgs 196/03.

1.3 Ambito di applicabilità

Queste Linee Guida si applicano a tutti i sottosistemi informativi aziendali, siano essi settoriali o centralizzati, che trattano dati critici per l'Azienda.

Non si applicano invece alle soluzioni informatiche "stand alone" installate nelle singole postazioni di lavoro dei reparti, dei servizi e/o dei laboratori o sulle postazioni di controllo di apparati medicali (oggetto di gestione dell'ingegneria clinica).

1.4 Documenti di riferimento

- Sistema Informativo Aziendale - Analisi dello stato delle risorse ICT - Piano triennale di sviluppo 2006-2008;

- DPS-LGR01 – Linee Guida per i Responsabili – per illustrare la tematica della privacy e della sicurezza e fornire indicazioni su come affrontarla e gestirla nella propria area di competenza;
- DPS-IST01 – Istruzioni per la Sicurezza dei Dati – per fornire indicazioni operative agli Incaricati sulle misure di sicurezza adottate per i trattamenti effettuati con strumenti elettronici;
- DPS-ISI02 – Registro Designazione Incaricati – per registrare l'avvenuta consegna agli incaricati delle istruzioni per applicare misure di sicurezza.

1.5 Acronimi e termini informatici utilizzati

- **ICT** – Information Communication Technologies: termine generico per indicare l'insieme delle infrastrutture e delle risorse informatiche hardware e software, che costituiscono la piattaforma sulla quale poggiano i sistemi informativi e i sistemi di comunicazione aziendali;
- **Backup** – termine generico che indica un'operazione periodica di copia dei dati per la loro conservazione per poterli riprendere per ripristinare i dati originari, in caso di perdita o distruzione degli stessi; esistono diverse modalità e forme di backup che rispondono a specifiche esigenze operative;
- **Restore** – operazione di ripristino dei dati originari partendo dalla copia effettuata con l'operazione di backup.
- **Vaulting** – particolare forma di operazione di backup, che presuppone che la copia dei dati venga conservata in un luogo diverso da quello dove risiede il sistema informatico oggetto dell'operazione di backup; anche in questo caso esistono diverse modalità e forme di vaulting; in particolare citiamo il vaulting su supporti rimovibili (nastri, cassette o CD/DVD) che vengono trasportati in un altro locale o sede, ed il vaulting elettronico effettuato direttamente su un'altra unità che risiede in un'altra sede, utilizzando le possibilità offerte dall'infrastruttura di rete;
- **DBMS** – Data Base Management System, termine che indica le tecnologie software e le risorse informatiche di sistemi specializzati per il supporto delle basi dati;
- **Snapshot** – letteralmente "scatto fotografico" o "fotografia"; termine comunemente usato per indicare un particolare tipo di backup che "fotografa" i dati così come sono in un particolare istante, senza interpretarne la struttura e coerenza logica;
- **Patch** - letteralmente "pezza di stoffa"; termine comunemente usato per indicare una modifica correttiva del software;
- **Unità di Storage** – termine generico per indicare un sistema ad accesso diretto, collegato in rete e specializzato per l'archiviazione e la gestione di grandi volumi di dati.

1.6 Struttura del documento

Il documento è strutturato nelle seguenti parti:

- **Generalità sulla Gestione dei Sistemi Informativi** – nella quale si descrive in che cosa consiste questo tipo di attività, gli attori coinvolti e i loro rispettivi ruoli, stabilendo un terminologia comune e fornendo linee guida operative, per uniformare la gestione dei sottosistemi informativi aziendali.
- **Considerazioni sull'affidabilità e la sicurezza dei Sistemi Informativi** – nella quale si affrontano tematiche e requisiti fondamentali per la configurazione e la gestione dei sottosistemi informativi aziendali;
- **Documentazione della Gestione dei Sistemi Informativi** – nella quale si descrive la documentazione da produrre durante la gestione dei sottosistemi informativi aziendali;
- **Compilazione del Libretto di Sistema** - nella quale si forniscono maggiori dettagli sui requisiti e sulle informazioni da fornire nella compilazione del Libretto di Sistema, perché possa essere utilizzato efficacemente per la gestione dei sottosistemi informativi aziendali.

2 Generalità sulla Gestione dei Sistemi Informativi

La **Gestione dei Sistemi Informativi** consiste nel presidio del sistema informatico che ospita le applicazioni ed i dati del sottosistema informativo aziendale e nell'esecuzione delle procedure operative previste, nei tempi e nei modi richiesti, con l'obiettivo di assicurare la continuità del servizio e il corretto trattamento dei dati.

Questa attività coinvolge diversi attori che interagiscono fra loro, nel rispetto del ruolo e delle competenze di ciascuno.

> ***Le attività di gestione dei sistemi informativi devono essere svolte solo da personale incaricato e espressamente autorizzato dal Responsabile dei Trattamenti dei Dati.***
>
> ***Materialmente le attività possono essere svolte sia dal personale dell'Azienda USL che da fornitori esterni, purché la supervisione complessiva resti di competenza dell'Azienda USL.***

Un presupposto essenziale per una corretta gestione dei sottosistemi informativi è la adeguata collocazione delle risorse informatiche (sistemi e apparati) in luoghi che siano:

- materialmente accessibili dalle sole persone autorizzate;
- in condizioni ambientali adeguate (temperatura, umidità, polvere, etc.) per garantire il corretto funzionamento delle apparecchiature;
- protetti, per quanto possibile, dal rischio d'incendio, di allagamento e di effrazione;
- eventualmente anche posti sotto gruppo di continuità, per assicurare il funzionamento dei sistemi informatici anche in caso di temporanea mancanza di alimentazione elettrica.

Nell'ambito del piano triennale di miglioramento delle risorse ICT dell'Azienda USL N. 1 è in corso di realizzazione un'azione specifica per concretizzare quanto prima le migliori condizioni per disporre di una adeguata localizzazione dei sottosistemi critici aziendali; tuttavia, in previsione della realizzazione di una vera e propria "server farm" aziendale, occorre fin d'ora che ciascun sottosistema informativo aziendale possa disporre di condizioni minime di sicurezza fisica tali da garantire la piena funzionalità e continuità operativa.

Gli interventi sui sistemi informatici possono essere pianificati (manutenzione ordinaria preventiva, migliorativa, adeguativa, etc.), oppure eseguiti a fronte di segnalazioni e specifiche esigenze (p.es. un malfunzionamento), e - a seconda dei casi - possono essere effettuati "on-site" o da remoto.

Nel caso delle attività affidate a fornitori esterni è necessario che siano definiti gli ambiti d'intervento ed il livello di servizio atteso, formulando contratti che prevedano accordi di servizio basati su indicatori e parametri quantificabili e monitorabili.

La documentazione della gestione dei sistemi informativi è un elemento essenziale per fornire un quadro preciso della situazione, e tracciare gli interventi effettuati e le attività svolte sui sistemi informativi, in modo da verificare e dimostrare che la loro gestione è conforme alle linee guida ed alle esigenze dell'Azienda USL.

Per maggiori dettagli sulle caratteristiche della documentazione da produrre, si faccia riferimento al capitolo 4 "*Documentazione della Gestione dei Sottosistemi Informativi*" a pagina 26.

2.1 Gli attori e i loro rispettivi ruoli

Nella gestione dei sottosistemi informativi aziendali dell'Azienda USL N. 1 intervengono i seguenti attori, ciascuno dei quali è identificato nel resto del documento con la rispettiva sigla tra parentesi:

- Responsabile del Settore Sistemi Informativi (RSSI)
- Responsabile dei Trattamenti (RT)
- Incaricato Gestione Sistema Informativo (IGSI)
- Responsabile Esterno (RE)

La figura seguente fornisce uno schema generale per esaminare i diversi attori, il loro ruolo e le possibili interazioni.

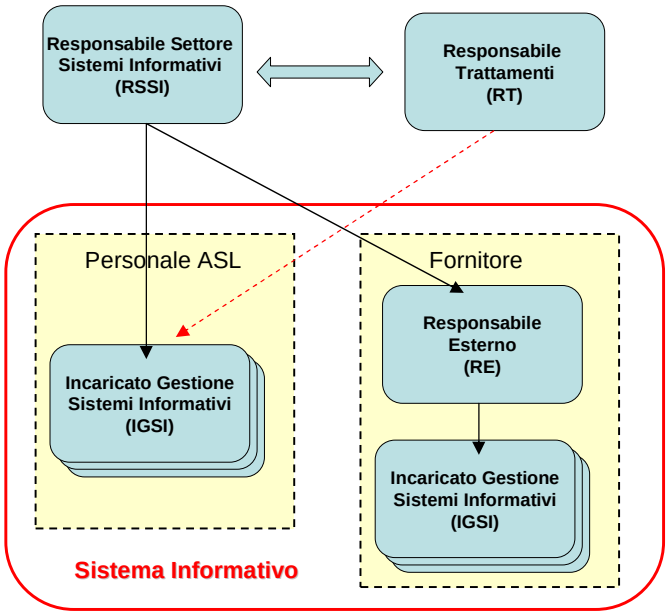

Figura 1- Attori che intervengono nella gestione dei sottosistemi informativi aziendali

Lo sviluppo e l'evoluzione dei sottosistemi informativi aziendali è coordinata dal **RSSI,** che collabora con i **RT,** per recepire le esigenze applicative e per realizzarle, nei limiti del mandato affidato dalla Direzione Generale e tenendo conto dell'evoluzione delle tecnologie ICT, dei prodotti applicativi esistenti sul mercato e dei requisiti funzionali degli utenti, nonché dell'evoluzione delle normative di legge e di settore.

A tendere, anche la gestione operativa (di natura sistemistica e non applicativa) dei sottosistemi informativi aziendali, dal punto di vista strettamente informatico (non applicativo) farà progressivamente capo al **RSSI**, che vi provvederà con propria struttura e/o con fornitori-consulenti esterni.

Tuttavia, attualmente i sottosistemi informativi aziendali dell'Azienda USL N. 1 sono per la maggior parte gestiti dai titolari del trattamento dei dati dei settori aziendali[2] (**RT**), ai quali

[2] Questi sono stati tutti nominati Responsabili dei Trattamenti (RT) dal Direttore Generale con le delibere n. 753 del 4/11/2004 e la n.830 del 22/11/2005.

sono stati nel tempo affidati per configurare gli strumenti necessari ad assolvere agli specifici adempimenti, siano essi settoriali o costituenti servizi applicativi centralizzati; ad esempio, per citarne solo alcuni:

- Il Servizio Personale;
- il Servizio Bilancio;
- il Centro Unico Prenotazione;
- il Servizio SAU;
- Il Servizio Sanità Animale;
- ecc..

In questo contesto, che viene definito necessariamente transitorio, gli **RT** mantengono quindi la piena responsabilità della gestione operativa dei sottosistemi informativi aziendali, collaborando e coordinandosi con il **RSSI,** per garantirne la conformità della gestione con queste linee guida.

Si tenga presente che in alcuni casi la gestione di sottosistemi informativi aziendali, anche se settoriali, sono affidati direttamente alla gestione del **RSSI**; tali sistemi sono per lo più componenti infrastrutturali (ad esempio: sistemi di accesso ad Internet, sistemi di gestione di reti di acquisizione dati, etc.).

Da un punto di vista operativo, sono gli **IGSI,** che materialmente intervengono sui sottosistemi informativi, in particolare sull'applicazione ed i dati, per svolgere le attività di gestione; tuttavia, essi svolgono la loro mansione sotto la supervisione di un responsabile competente (**RT**).

E' compito del responsabile competente **RT** nominare, sentito il **RSSI**, gli **IGSI**, individuando l'ambito delle loro competenze, ed impartendo loro le istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati, tenuto conto delle presenti linee guida.

E' altresì compito del responsabile **RT** verificare e garantire che i risultati dell'operato degli **IGSI**, che a lui riferiscono, siano conformi alle linee guida e al livello di servizio stabilito per il sottosistema informativo aziendale di cui trattasi.

Nel caso in cui gli **IGSI** siano dipendenti dell'Azienda USL (o assimilabili: collaboratori esterni, lavoro interinale, etc.), la loro nomina viene effettuata dal dirigente del settore di appartenenza:

dal **RSSI**, se gli **IGSI** fanno parte dell'organico del **SSI**;

dal **RT** che è responsabile della gestione operativa del sottosistema informativo, se gli **IGSI** fanno parte dell'organico di quel settore.

Nel caso in cui le attività siano svolte da soggetti esterni (uno o più fornitori), è necessario che i fornitori ai quali vengono affidati i servizi indichino il nominativo della loro persona di riferimento, che supervisionerà e coordinerà le attività del personale incaricato di effettuare gli interventi richiesti; questa persona sarà nominata Responsabile Esterno **(RE)** dal **RSSI,** e sarà responsabile delle attività svolte dai suoi collaboratori (**IGSI**).

Ogni **RE** deve predisporre e mantenere aggiornato l'elenco dei propri **IGSI**, che materialmente opereranno sui sistemi informativi, comunicandolo al **RSSI** ed assicurando che ogni **IGSI** conosca l'ambito di riferimento del proprio incarico e le disposizioni dell'Azienda USL in merito alla tutela della privacy e della sicurezza dei dati.

Per supportare il compito dei vari responsabili e degli incaricati, sono stati predisposti i seguenti documenti di riferimento:

- **DPS-LGR01 – Linee Guida per i Responsabili** – per illustrare la tematica della privacy e della sicurezza e fornire indicazioni su come affrontarla e gestirla nella propria area di competenza;
- **DPS-IST01 – Istruzioni per la Sicurezza dei Dati** – per fornire indicazioni operative agli Incaricati sulle misure di sicurezza adottate per i trattamenti effettuati con strumenti elettronici;
- **DPS-IST02 – Registro Designazione Incaricati** – per registrare l'avvenuta consegna agli incaricati delle istruzioni per applicare misure di sicurezza.

Seguono maggiori dettagli sui vari attori.

2.1.1 Responsabile del Settore Sistemi Informativi (RSSI)

Il Settore Sistemi Informativi è la struttura responsabile dell'infrastruttura di rete e dell'integrazione dei sottosistemi informativi aziendali.

Il dirigente Responsabile del **SSI** è nominato Responsabile della Sicurezza Informatica (Delibera n. 831 del 22/11/2005) e, in quanto tale è il punto centrale di raccordo con tutti gli altri Responsabili dei Trattamenti, per ottemperare agli adempimenti prescritti dal D. Lgs. 196/2003.

In tale ambito, egli ha il compito di:

- censire le caratteristiche aggiornate dei sottosistemi informativi aziendali, dei trattamenti con essi effettuati, delle misure di sicurezza adottate e dell'organizzazione delle competenze per la loro gestione;
- analizzare e valutare i rischi che gravano sui dati informatizzati e sugli strumenti, identificando di conseguenza gli elementi da proteggere e le minacce cui essi sono sottoposti;
- sulla base dell'analisi dei rischi, definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi elettronici di dati personali, delle procedure e dei sistemi informativi esistenti, osservando quanto prescritto dal Dlgs 196/2003 e dal relativo disciplinare tecnico allegato sub B);
- definire e progressivamente realizzare e migliorare il sistema di sicurezza dei sistemi informativi e dell'infrastruttura informatica aziendale, in base ai requisiti definiti nel punto precedente;
- pianificare gli interventi di monitoraggio della sicurezza e di predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate;
- assicurarsi che siano adeguatamente predisposti e mantenuti in efficienza i sistemi e le procedure di ripristino dei dati;
- assicurarsi che sia effettuata la manutenzione e l'aggiornamento degli strumenti di protezione informatica, per assicurarne la costante efficienza, disponibilità e adeguatezza far fronte alle nuove minacce;
- assicurarsi che i soggetti esterni, cui l'Azienda dovesse affidare il trattamento di dati personali informatizzati, adottino misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal relativo disciplinare tecnico, allegato sub B) al Dlgs 196/2003 stesso.

Come tutti i Responsabili dei Trattamenti nominati dalla Direzione, il **RSSI** ha la responsabilità di nominare gli Incaricati **IGSI**, ovvero i collaboratori dipendenti o

assimilabili, ai quali vengono affidati i trattamenti della propria area di pertinenza, individuando gli ambiti dei trattamenti ad essi affidati, ed impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati.

Qualora il **RSSI** si avvalga di fornitori esterni per svolgere le attività di competenza, è sua responsabilità individuare e nominare i Responsabili Esterni (**RE**) ai quali indicherà l'ambito dei trattamenti affidati e le disposizioni dell'Azienda USL N.1 Sassari per adozione delle misure di sicurezza, di tutela e di garanzia dei dati.

2.1.2 Responsabile Trattamenti (RT)

Per ogni sottosistema informativo aziendale deve essere individuabile almeno un **RT**, ossia la persona responsabile di una struttura aziendale semplice o complessa, che sia utente principale del sottosistema informativo, col quale il **RSSI** possa collaborare per supportare la gestione e per recepire e consolidare i requisiti funzionali della soluzione informatica migliore per le esigenze di quel settore.

Nell'ambito degli adempimenti di Legge sulla Privacy (Delibere n. 753 del 4/11/2004 e la n. 830 del 22/11/2005), il dirigente della struttura (o un responsabile delegato dalla Direzione Generale) è nominato Responsabile dei Trattamenti dei Dati effettuati con il sottosistema informativo in dotazione; in tale veste egli ha la responsabilità di:

- nominare gli Incaricati, ovvero i collaboratori dipendenti o assimilabili, ai quali vengono affidati i trattamenti dei dati di pertinenza, individuando gli ambiti dei trattamenti a loro affidati ed impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati;
- verificare almeno semestralmente lo stato di applicazione delle direttive dell'Azienda USL, nonché la corretta applicazione delle misure di sicurezza e riferendo al **RSSI**;
- verificare almeno semestralmente l'aggiornamento della lista degli incaricati dei trattamenti effettuati con il sottosistema informativo e la sussistenza dei presupposti per la definizione dei loro profili di autorizzazione, comunicando le eventuali variazioni al **RSSI**.

Qualora il **RT** abbia anche la responsabilità della gestione operativa del sottosistema informativo in dotazione, egli deve adottare le misure di sicurezza idonee alla sensibilità dei dati trattati col sottosistema informativo, applicando le linee guida e le disposizioni del **RSSI** in materia di sicurezza informatica e tutela dei dati aziendali. A lui spetta in particolare:

- nominare gli **Incaricati della Gestione Sistemi Informativi (IGSI)**, ovvero i collaboratori dipendenti o assimilabili, ai quali vengono affidate le attività di gestione operativa dei sistemi e delle risorse informatiche in dotazione, individuando gli ambiti di competenza a loro affidati e impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati;
- assicurarsi che la documentazione richiesta, per la gestione del sottosistema informativo, sia corretta, completa e costantemente aggiornata, secondo le indicazioni ricevute dal **RSSI**.
- certificare gli interventi effettuati o ottenere la certificazione di conformità dal fornitore, nel caso di interventi eseguiti da terzi;

- effettuare le verifiche periodiche della sussistenza delle condizioni per l'abilitazione degli incaricati all'uso del sottosistema informativo;

trasmettere al **RSSI** i nominativi degli **IGSI** da lui nominati e la documentazione aggiornata del sottosistema informativo gestito;

interagire con il RSII per la segnalazione delle esigenze applicative e di modifica delle configurazioni dei sistemi informatici in dotazione.

2.1.3 Incaricato Gestione dei Sistemi Informatici (IGSI)

E' una persona interna (collaboratore dipendente o assimilato) o esterna all'Azienda, al quali vengono affidate le attività per la manutenzione, la gestione e l'adozione delle misure di sicurezza dei sistemi informatici e dell'infrastruttura di rete (in quest'ultimo caso previa autorizzazione del **RSSI**).

Gli incaricati della gestione dei sistemi informativi sono nominati dal rispettivi responsabili; essi sono tenuti ad operare rispettando gli ambiti delle competenze a loro affidate e adottando le modalità operative a loro indicate per l'espletamento dei compiti assegnati.

2.1.4 Responsabile Esterno (RE)

Qualora ci si avvalga di soggetti esterni per gestire il sottosistema informativo, è necessario che i fornitori ai quali vengono affidati i servizi, indichino il nominativo della persona di riferimento, che coordinerà le attività del personale incaricato di effettuare gli interventi richiesti.

Nella generalità dei casi i rapporti con i fornitori esterni vengono intrattenuti centralmente dal RSSI, con l'intento di coordinare le misure di sviluppo e miglioramento del sottosistema informativo aziendale nel suo complesso, nonché di garantire adeguate economia di scala e standard operativi comuni.

Il **RSSI** provvede quindi alla nomina del **Responsabile Esterno (RE),** per ciascun fornitore e per ciascun specifico sottosistema informativo aziendale, specificando l'ambito di competenza degli interventi sul sottosistema informativo e fornendo le linee guida e le direttive aziendali per la corretta esecuzione delle prestazioni richieste.

Il **RE** deve far rispettare ai suoi collaboratori le disposizioni ricevute dal **RSSI**, rispondendo della corretta applicazione delle linee guida e delle disposizioni del **RSSI** in materia di sicurezza informatica e tutela dei dati aziendali. A lui spetta:

- coordinare i propri dipendenti/collaboratori, nominandoli **Incaricati della Gestione Sistemi Informatici (IGSI)**, individuando gli ambiti di competenza di ciascuno e impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati;
- comunicare al **RSSI** i nominativi degli **IGSI** da lui nominati;
- assicurarsi che gli interventi effettuati sui sistemi informativi di competenza, siano conformi alle indicazioni del **RSSI** in materia di sicurezza informatica e tutela dei dati aziendali;
- fornire al **RSSI** la certificazione di conformità degli interventi eseguiti sui sistemi.

2.2 Classificazione delle attività per area di competenza

La figura mostra un quadro generale di riferimento delle attività di gestione e supporto di un generico sottosistema informativo, utilizzando la terminologia e la notazione adottata dal CNIPA[3].

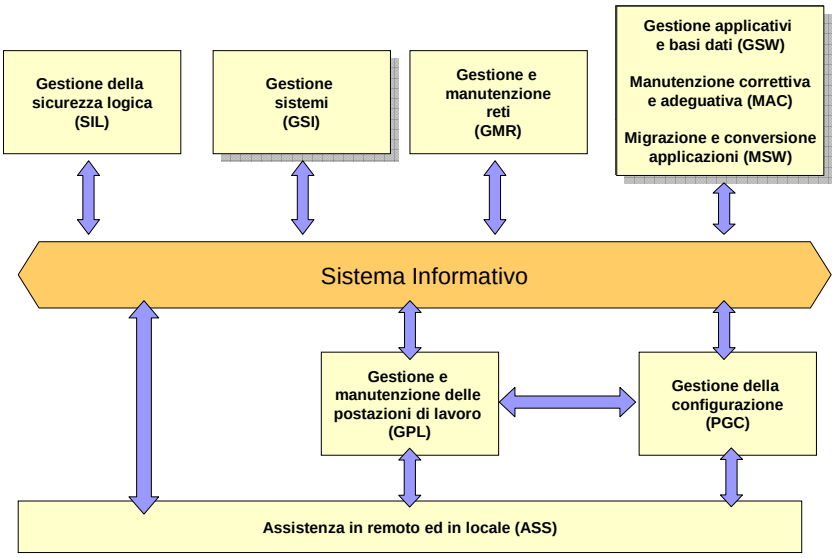

Figura 2 - Classificazione attività secondo il modello CNIPA

In essa sono evidenziate quelle attività che, a seconda dei casi, possono essere di competenza del **RSSI** o del **RT;** mentre le restanti sono tutte di competenza del **RSSI**.

In queste Linee Guida saranno discusse le attività operative evidenziate; ossia:

- Gestione dei Sistemi (GSI)
- Gestione dell'Applicativi e Basi Dati (GSW)[4]
- Manutenzione correttiva ed adeguativi (MAC)
- Migrazione e conversione applicazioni (MSW)

2.2.1 Gestione dei Sistemi (GSI)

La **GSI** si occupa della gestione della configurazione delle risorse informatiche (hardware e software di base) e delle risorse di rete utilizzate dal sottosistema informativo per garantire la sicurezza, l'affidabilità e la continuità di servizio della piattaforma tecnologica sulla quale poggia.

In questo ambito rientrano tutti gli interventi e le attività concernenti la piattaforma tecnologica del sottosistema informativo; in particolare:

[3] Il codice tra parentesi è quello adottato dal CNIPA
[4] Nella figura la GSW è generalmente ricompressa in GSI, ma in questo contesto si è preferito evidenziarla a parte.

- la gestione[5] della configurazione delle componenti hardware dei sistemi e della rete, del software di base e di supporto, per rispondere ai requisiti di affidabilità, disponibilità e sicurezza dell'Azienda USL N. 1 di Sassari;
- il monitoraggio e l'ottimizzazione delle prestazioni dei sottosistemi informativi aziendali, con particolare riferimento alla rete ed alle infrastrutture hardware;
- il monitoraggio, la gestione della disponibilità, la pianificazione del miglioramento dell'affidabilità e della sicurezza fisica e perimetrale delle risorse informatiche in dotazione[6];
- la pianificazione e l'esecuzione degli interventi di manutenzione preventiva e di aggiornamento del software di base ed applicativo, nonché dell'hardware della piattaforma tecnologica del sistema (previo accordo con il **RSSI**);
- la pianificazione e l'esecuzione degli interventi di manutenzione preventiva delle componenti hardware e software di base degli impianti di pertinenza;
- l'attivazione delle configurazioni d'emergenza e la tempestiva riattivazione del servizio, in caso di interruzioni dovute a guasti o malfunzionamento della piattaforma tecnologica;
- l'attivazione ed il controllo dell'esecuzione degli interventi di riparazione delle componenti hardware e degli impianti di pertinenza;
- l'aggiornamento e l'applicazione di patch al software di base e di supporto;
- la supervisione della gestione dei tentativi di recupero di dati dai supporti danneggiati, qualora disponibili i backup effettuati come dalle presenti linee guida di gestione.

Nello svolgimento dell'attività il responsabile del sottosistema informativo **RT** utilizza servizi di supporto sistemistico, coordinati da **RSSI**, per intervenire su richiesta, o in modo pianificato, sulla configurazione del software di sistema e di rete, al fine di:

- ottimizzare l'uso delle risorse o per migrare su una piattaforma tecnologica più aggiornata;
- risolvere tempestivamente i problemi riferibili alla piattaforma tecnologica software.

Questo servizio, utilizzato in base alle necessità, consente di gestire correttamente la configurazione delle componenti software di base dei sistemi hardware e delle eventuali reti locali e per:

- l'analisi e la risoluzione dei problemi riferibili alla piattaforma tecnologica assegnata;
- l'applicazione di patch al software di base;
- il tentativo di recupero di dati da supporti danneggiati;
- l'installazione, l'aggiornamento della configurazione del software e degli strumenti di monitoraggio e controllo della sicurezza;
- l'analisi e l'ottimizzazione delle prestazioni dei sistemi e della rete, da effettuarsi in stretta collaborazione con il **SSI**, responsabile della gestione dell'intera rete aziendale.

[5] Gli aggiornamenti della configurazione sono programmati dal RSSI in collaborazione con gli RT utenti del sottosistema informativo
[6] La pianificazione del miglioramento andrà pianificata in collaborazione con il RSSI

- Le richieste d'intervento devono essere servite nei tempi e nei modi previsti dalle presenti linee guida, con particolare riferimento agli Accordi di Servizio con i fornitori.

E' opportuno che le richieste di intervento siano tracciate e che sia sempre aggiornato il loro stato di completamento.

E' anche necessario che gli interventi di modifica effettuati sui sistemi informativi siano registrati su un apposito **Giornale di Gestione Configurazione[7].**

> ***In particolare, per gli interventi che comportano modifiche alla configurazione, è necessario che sia fornita una certificazione di conformità con le norme di sicurezza previste dal D. Lgs 196/03.***

2.2.2 Gestione dell'Applicazione e della Base Dati (GSW)

La **GSW** comprende le attività operative richieste dall'applicazione vera e propria; ossia:

- la gestione operativa
- la gestione dei dati
- la gestione degli utenti

E' necessario che tutte le attività eseguite dagli **IGSI** siano tracciate in un apposito **Giornale di Gestione Applicazione[8].**

> ***E' necessario che per ciascun tipo di attività sia individuato un IGSI (eventualmente la stessa persona può avere più di un incarico)***

Gestione operativa

E' l'insieme delle attività che servono per mantenere operativo il servizio agli utenti; come ad esempio le attività di:

- attivazione, disattivazione e ripartenza programmata dell'applicazione;
- monitoraggio della disponibilità dell'applicazione e ripristino dell'operatività quando è necessario;
- monitoraggio delle attività automatizzate e intervento in caso di anomalie;
- schedulazione e verifica delle procedure di elaborazione massiva dei dati;
- gestione dei flussi di interfaccia da e verso altri sistemi informativi;
- produzione di report di rendiconto sulla disponibilità e sulle prestazioni dell'applicazione;
- supporto della di manutenzione correttiva e di quella evolutiva[9] del software applicativo.

[7] Si veda il capito 4 "Documentazione della Gestione dei Sistemi Informativi"
[8] Si veda il capito 4 "Documentazione della Gestione dei Sistemi Informativi"
[9] Come concordata con il RSSI.

Gestione dei Dati

Si tratta delle attività operative di amministrazione del DBMS e dello "Storage" per assicurane la l'efficienza, l'integrità e la disponibilità. In particolare in quest'area rientrano ad esempio le attività di:

- amministrazione dello spazio utilizzato per memorizzare i dati sul DBMS e sullo Storage;
- amministrazione degli archivi e degli indici per recuperare lo spazio inutilizzato e garantire le migliori prestazioni nell'accesso ai dati;
- monitoraggio delle procedure automatizzate di salvataggio e intervento in caso di necessità;
- schedulazione e verifica delle procedure di backup di vaulting dei dati su supporti esterni, per poterli ripristinare in caso di necessità;
- recupero e ripristino dei dati in caso di necessità;
- monitoraggio e verifica dell'affidabilità dei dispositivi di memorizzazione dei dati e intervento in caso di necessità;
- pianificazione, coordinamento e supporto della manutenzione correttiva ed evolutiva dei sistemi di memorizzazione dei dati e del software di supporto della loro gestione.

Gestione degli Utenti

La gestione degli utenti comprende tutte le attività connesse con amministrazione degli utenti e delle loro credenziali di accesso al sottosistema informativo; ad esempio:

- la definizione e la gestione delle credenziali di autenticazione e di autorizzazione degli Utenti all'uso dell'applicazione
- la definizione dei profili di autorizzazione coerenti con le disposizioni del Responsabile dei Trattamenti, per delimitare gli ambiti d'azione degli Incaricati;
- l'impostazione delle politiche di verifica della validità e della scadenza delle password;
- l'assegnazione di credenziali temporanee per abilitare incaricati esterni all'esecuzione degli interventi di manutenzione del sottosistema informativo;
- la produzione di report per supportare il **RT** e il **RSSI** nella verifica periodica di sussistenza delle condizioni per l'accesso all'applicazione da parte degli Utenti registrati.

2.2.3 Manutenzione Correttiva (MAC)

E' l'attività di manutenzione correttiva del software applicativo a fronte delle anomalie riscontrate sia durante il periodo di garanzia che successivamente.

L'obiettivo fondamentale è di risolvere tempestivamente i problemi segnalati dagli utenti e dagli operatori del sottosistema informativo.

L'attività consiste in:

- la riproduzione dell'anomalia segnalata in ambiente di test;

- l'analisi e la risoluzione dei problemi riferibili al software applicativo e ai dati del sottosistema informativo;
- lo sviluppo e il test di "patch" al software applicativo
- l'aggiornamento eventuale della documentazione tecnica
- il recupero e il ripristino dei dati applicativi eventualmente danneggiati dall'anomalia riscontrata
- la messa in produzione della modifica al software e presa in carico da parte del responsabile della gestione operativa dell'applicazione.

Le richieste d'intervento devono essere servite nei tempi e nei modi previsti dall'accordo di servizio.

E' opportuno che:

- Le segnalazioni siano registrate e classificate in base alla criticità indicata dall'utente e alla priorità che il responsabile della gestione operativa dell'applicazione può impostare.
- Le segnalazioni siano servite in base alla priorità , alla criticità e all'anzianità della segnalazione
- le richieste di intervento siano tracciate e che sia sempre aggiornato il loro stato di completamento;

E' necessario che gli interventi correttivi effettuati siano registrati nel **Giornale di Gestione Configurazione.**

Per gli interventi che comportano modifiche alla configurazione sia fornita una certificazione di conformità con le norme di sicurezza

2.2.4 Migrazione e conversione applicazione (MSW)

E' un'attività coordinata dal **RSSI** per rispondere tempestivamente all'evoluzione delle tecnologie ICT e dei requisiti funzionali dei Responsabili dei Trattamenti, degli utenti o all'evoluzione delle normative che governano gli algoritmi dell'applicazione;

L'attività consiste in:

- L'analisi de requisiti e definizione delle specifiche da soddisfare
- La definizione e lo sviluppo della soluzione
- Il test del software applicativo sviluppato
- l'aggiornamento eventuale della documentazione tecnica e per l'utente
- l'eventuale migrazione dei dati all'atto della messa in produzione del nuovo software
- la messa in produzione del software applicativo e la presa in carico da parte del responsabile della gestione operativa dell'applicazione
- La formazione degli utenti e degli operatori ad usare correttamente il sistema e/o l'apparato in dotazione

Le esigenze e le richieste vengono raccolte ed esaminate da **RSSI** che provvede a raggrupparle in progetti in base a criteri di opportunità concordati con i Responsabili dei Trattamenti (**RT**), che si avvalgono del sottosistema informativo per lo svolgimento della loro attività

RSSI provvede anche a monitorare e a tracciare lo stato d'avanzamento dei progetti fino alla messa in produzione del nuovo sistema o della nuova versione del software applicativo.

La programmazione dei progetti e il controllo del loro stato d'avanzamento è effettuato da **SSI** nel **Programma di Sviluppo**[10]

E' necessario che quando viene messo in produzione il nuovo sistema, l'evento sia registrato nel **Giornale di Gestione Configurazione** del sottosistema informativo.

Per gli interventi che comportano modifiche al sistema di sicurezza è necessario che il fornitore certificazione la conformità con le norme di sicurezza.

2.2.5 Assistenza Tecnica (ASS)

RSSI assicura un servizio specialistico centralizzato per l'assistenza tecnica e la manutenzione degli apparati e dei sistemi hardware dell'infrastruttura della rete e dei sistemi informatici utilizzati dal sottosistema informativo.

Il servizio ha l'obiettivo di prevenire i guasti o di intervenire tempestivamente sistemi e gli apparati hardware per:

- l'analisi e la risoluzione dei problemi riferibili alle sole componenti hardware e all'eventuale firmware di corredo.
- La sostituzione dei dispositivi difettosi (hardware e/o firmware)
- L'installazione di nuovi dispositivi e/o eventuali nuovi firmware
- La formazione degli utenti e degli operatori ad usare correttamente il sistema e/o l'apparato in dotazione
- Il recupero di dati da sistemi ormai inutilizzabili

Gli interventi devono essere pianificati e serviti nei tempi e nei modi concordati col fornitore.

E' opportuno che:

- gli interventi preventivi siano pianificati sulla base delle esigenze di continuità di servizio;
- gli interventi su chiamata siano eseguiti nei tempi e nei modi pattuiti con il fornitore;
- tutti gli interventi effettuati siano tracciati in un apposito registro da esibire;
- sia richiesta al fornitore la certificazione di conformità con le norme di sicurezza.

[10] Si veda il capito 4 "Documentazione della Gestione dei Sistemi Informativi"

3 Considerazioni sull'affidabilità e la sicurezza del sottosistema informativo

3.1 L'affidabilità intrinseca e la tolleranza ai guasti

Un primo elemento di riferimento da considerare per valutare l'adeguatezza di un sistema è la sua intrinseca affidabilità e capacità di tollerare i guasti, che gli deriva dal tipo e dalla configurazione delle componenti hardware e del software di base.

In questo ambito gli approcci sono vari, dipendono dai requisiti di affidabilità espressi dagli **RT,** utenti del sottosistema informativo, e si basano caso per caso su una combinazione di strategie, delle quali le più frequenti sono:

- utilizzo di componenti hardware ad alta affidabilità intrinseca, che supportano Hot-Swap per la sostituzione delle parti difettose senza spegnere il sistema;
- utilizzo di sistemi specializzati per lo "storage dei dati" altamente affidabili e performanti, come ad esempio SAN e NAS, che gestiscono efficacemente ed efficientemente le funzioni automatiche di Backup e electronic Vaulting.dei dati
- disponibilità di risorse hardware e di connessioni ridondanti o di riserva da utilizzare in caso di emergenza
- configurazione delle risorse in modalità active/active o active/passive per supportare il monitoraggio della funzionalità delle componenti, segnalazione delle anomalie e il subentro in caso di guato di una componente del sistema;
- utilizzo di strumenti e procedure automatiche o manuali per l'effettuare lo switch-over in caso guasto di una risorsa, con o senza interruzione del servizio.
-

> ***La descrizione dell'architettura del sottosistema informativo dovrà evidenziare se e come questi aspetti sono stati presi in considerazione nella progettazione della soluzione informatica.***

3.2 La sicurezza fisica

E' l'insieme delle misura di sicurezza che hanno il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento del lavoro con gli strumenti automatizzati: la protezione delle aree e dei locali, in cui sono situati gli elaboratori; deve essere quindi attivata sia contro eventi dannosi imprevedibili (inondazioni, corti circuiti, ecc.), che contro tentativi di intrusione.

> ***Nel contesto specifico, l'obiettivo primario è di proteggere le apparecchiature e i dati da eventi di natura accidentale (es. incendi, allagamenti, etc.) e da intrusioni di personale non autorizzato o di terzi, che potrebbero sottrarre, manomettere o danneggiare i sistemi e i dati con essi trattati.***

In quest'ambito le misure riguardano:

- l'ubicazione dei sistemi in locali idonei, protetti e sorvegliati;

- la collocazione delle stazioni di lavoro;
- il salvataggio dei dati;
- la custodia e archiviazione dei supporti rimovibili dei dati.

3.2.1 L'ubicazione dei sistemi e degli apparati della piattaforma tecnologica

A livello generale i sistemi informatici e gli apparati di rete non devono essere situati in locali aperti al pubblico, senza presidio e senza un'adeguata protezione che impedisca agli estranei di asportarli, di danneggiarli, di manometterli e nemmeno di vedere i dati trattati, all'insaputa dell'incaricato.

Sarebbe opportuno pertanto che i sistemi e gli apparati di rete dei sistemi informativi siano situati in un apposito "Data Center", accessibile solo dal personale autorizzato, ossia in un locale dedicato, adeguatamente attrezzato e protetto per:

- assicurare le condizioni ambientali (temperatura, umidità e purezza dell'aria) ottimali per il buon funzionamento degli apparati e dei sistemi informatici;
- controllare l'accesso al locale da parte di chiunque, bloccando le persone non autorizzate;
- segnalare tempestivamente le condizioni ambientali anomale e i tentativi di effrazione;
- intervenire automaticamente in caso di incidente (es. incendio, allagamento) per circoscrivere e contenere il danno.
-

> ***Nel caso la gestione del sottosistema informativo non comporti la necessità di un presidio continuo, è opportuno che il Data Center sia anche sottoposto a Video Sorveglianza, in particolare al di fuori del normale orario di lavoro.***

Nell'ambito del piano triennale di miglioramento delle risorse ICT dell'Azienda USL N. 1 è in corso di realizzazione un'azione specifica per concretizzare - quanto prima - le migliori condizioni per disporre di una adeguata localizzazione dei sottosistemi critici aziendali; tuttavia, in previsione della realizzazione di una vera e propria "Server Farm" aziendale (o "Data Center"), occorre fin d'ora che ciascun sottosistema informativo aziendale possa disporre di condizioni minime di sicurezza fisica tali da garantire la piena funzionalità e continuità operativa.

3.2.2 La collocazione delle stazioni di lavoro

A livello generale i sistemi informatici e gli apparati di rete non devono essere situati in locali aperti al pubblico, senza presidio e senza un'adeguata protezione che impedisca agli estranei di asportarli, di danneggiarli, di manometterli e nemmeno di vedere i dati trattati, all'insaputa dell'incaricato.

La collocazione delle stazioni di lavoro deve essere tale da assicurare anche che:

- anche in presenza dell'incaricato, le persone non autorizzate non possano vedere le informazioni visualizzate sullo schermo e non possano accedere alla tastiera e al mouse;
- in assenza dell'incaricato la stazione di lavoro sia oscurata e disabilitata;

3.2.3 Il salvataggio dei dati

E' necessario minimizzare il rischio di perdita dei dati critici anche in caso di eventi catastrofici, pertanto anche se le attuali tecnologie utilizzate sono altamente affidabili e tolleranti ai guasti, è opportuno adottare delle adeguate strategie che garantiscano la disponibilità di un copia dei dati critici anche in un'altra sede, per poterli recuperare anche in casi di disastro.

Una possibile strategia è la seguente:

- memorizzare i dati su unità Storage ad alta capacità e al alta affidabilità (es. NAS o SAN) che centralizza i servizi di memorizzazione di massa e di backup;
- su questa unità attivare un sistema di backup che provvede ad effettuare automaticamente su se stesso degli snapshot a caldo più volte al giorno (es. 4 o 6 volte) senza impattare sull'operatività del sistema;
- è possibile utilizzare anche le funzionalità del DBMS per effettuare sempre a caldo dei backup logici della Base Dati anche più volte al giorno;
- usando gli snapshot e i backup logici disponibili sull'unità di storage è possibile schedulare delle procedure di "Vaulting" anche giornaliere, su un supporto rimovibile da portare in altra sede, o direttamente su un'altra unità di storage (NAS o SAN) installata in un'altra sede, utilizzando una connessione di rete.

> ***In quest'ultimo caso si dirà che si sta usando una procedura di "electronic vaulting"***

3.2.4 Custodia e archiviazione della documentazione dei supporti rimovibili dei dati

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti removibili di memorizzazione dei dati (ad esempio Tape, CD, dischetti, ecc.), è opportuno disporre di armadi e schedari, chiudibili a chiave, nei quali riporre i documenti e i supporti rimovibili dei dati.

3.3 La sicurezza logica

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si riassumono di seguito le misure che è necessario adottare:

- utilizzo di un **sistema di autenticazione informatica**, che ha il fine di accertare l'identità delle persone atte a svolgere un determinato trattamento, in modo che possano accedere ai dati personali le sole persone autorizzate;
- utilizzo di un **sistema di autorizzazione**, che ha il fine di circoscrivere le tipologie di dati ai quali gli Incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative;
- gestione di un **sistema di protezione**, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);
- prescrizione delle **opportune cautele per la custodia e l'utilizzo** dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

3.3.1 La disattivazione delle credenziali di autorizzazione

Al verificarsi dei seguenti casi, è necessario procedere alla disattivazione delle credenziali di autorizzazione:

- immediatamente, nel caso in cui l'Incaricato perda la qualità che gli consentiva di accedere allo strumento (p.es. cessazione del rapporto di lavoro con l'Azienda);
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

3.3.2 I profili di autorizzazione

Per discriminare le tipologie di dati ai quali ciascun incaricato può accedere, ed i trattamenti che può effettuare, si deve impostare un sistema di autorizzazione che circoscriva la sfera d'azione di ciascuno ai dati ed ai trattamenti strettamente necessari per lo svolgimento delle proprie mansioni lavorative.

L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun Incaricato o di ciascuna classe omogenea di Incaricati, ai soli dati necessari per effettuare le operazioni di trattamento che sono indispensabili per svolgere le mansioni lavorative.

3.3.3 La verifica periodica di sussistenza

Periodicamente, e comunque almeno annualmente, deve essere verificata la sussistenza delle condizioni per la conservazione delle credenziali di autorizzazione che siano coerenti con l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

3.3.4 La protezione anti-intrusione e anti-virus

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi antivirus che contengono codici maliziosi (virus, trojan, backdoor, etc.), devono essere adottati idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento più frequente per i sottosistemi informativi aziendali.

Occorre provvedere anche alla protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall e anti-spyware.

A tale riguardo l'Azienda USL N. 1 è dotata di più firewalls che limitano l'accesso alla rete aziendale dall'esterno a servizi e utenti non autorizzati.

Inoltre sono impartite istruzioni ai responsabili RT dei vari sottosistemi di tenersi aggiornati periodicamente sui programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne eventuali difetti (fix, patch, service pack, ecc.).

3.3.5 La gestione dei supporti fisici rimovibili

Per quanto concerne i supporti fisici rimovibili (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, è necessario che:

- i supporti siano custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati o distrutti, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

4 Documentazione della Gestione dei Sottosistemi Informativi

Come già detto, la documentazione è essenziale; in questo capitolo vendono illustrati i documenti richiesti per fornire un quadro preciso della situazione ed assicurare una corretta gestione operativa dei sottosistemi informativi, tracciando gli interventi effettuati e le attività svolte.

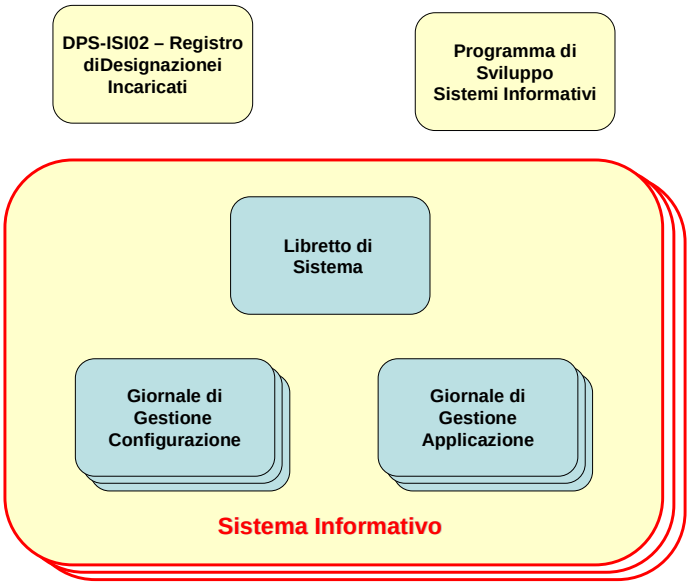

Figura 3 - Documentazione di Gestione Sistemi Informativi

La figura fornisce una panoramiche dei documenti richiesti per ogni sottosistema informativo:

- Il **Libretto di Sistema** dove sono documentate le caratteristiche generali del sottosistema informativo che sono rilevanti per la sua gestione;
- Il **Giornale di Gestione Configurazione** dove è tracciata la storia delle modifiche della configurazione hardware, software e di rete del sottosistema informativo;
- Il **Giornale di Gestione Applicazione** sono tracciati tutte le attività di gestione operativa dell'applicazione, dei dati e degli utenti effettuati dagli IGSI;

A questi documenti, si aggiungono il **DPS-ISI02 – Registro Designazione Incaricati**, che ogni RT deve tenere per annotare le nomine degli incaricati e dei responsabili esterni effettuate nel settore di propria competenza, e il **Programma di Sviluppo Sistemi Informativi**, che è tenuto dal dirigente responsabile del **SSI**.

Fatta eccezione del **DPS-ISI02 – Registro Designazione Incaricati**, che è già noto in base alle precedenti documentazioni prodotte, di seguito vengono illustrati i contenuti di tutti questi documenti.

4.1 Libretto di Sistema

4.1.1 Scopo

Per ogni sottosistema informativo è necessario predisporre un **Libretto di Sistema**, che documenti in modo uniforme le caratteristiche generali che sono rilevanti per monitorare e supportare centralmente la sua gestione e mantenere sempre aggiornato il Documento Programmatico sulla Sicurezza.

L'obiettivo è di disporre di un quadro aggiornato della situazione dei sottosistemi informativi aziendali dell'Azienda USL e di come questi siano gestiti, e per poter più facilmente pianificarne l'evoluzione, la razionalizzazione e il miglioramento.

Il documento non è una replica o un sostituto della documentazione tecnica e operativa di corredo del sottosistema informativo, bensì è una "fotografia" standard delle caratteristiche generali del sottosistema informativo e di come esso viene gestito.

4.1.2 Descrizione dei contenuti

E' stato predisposto un modello Word (**SSI-m01)** per aiutare a redigere questo tipo di documento seguendo uno schema strutturato nelle seguenti sezioni:

- Intestazione
- Sezione A – Finalità del Sottosistema Informativo e Organizzazione di Supporto
- Sezione B – Architettura e Logistica della piattaforma tecnologica
- Sezione C – Politiche di Gestione del Servizio
- Sezione D – Livello di Servizio garantito
- Sezione E – Attestazione di conformità delle misure di sicurezza

Per maggiori dettagli si rimanda al succitato modello e alla parte "*Compilazione del Libretto di Sistema*".

4.1.3 Gestione del documento

Il documento deve essere compilato e pubblicato a cura del responsabile della gestione operativa del sottosistema informativo, ed una copia elettronica deve essere inviata al **RSSI** perché ne prenda atto e archivi l'edizione consolidata del documento, come riferimento del sottosistema informativo censito.

Il responsabile della gestione del sottosistema informativo **RT** assicura che il Libretto di Sistema sia sempre aggiornato per riflettere la situazione corrente, facendovi riportare le modifiche intervenute nel frattempo e pubblicando sistematicamente le nuove edizioni aggiornate.

Tutte le copie elettroniche consolidate sono archiviate dal **RSSI** che assicura che l'edizione corrente sostituisca l'edizione precedente.

4.2 Programma di Sviluppo

4.2.1 Scopo

Il **RSSI** mantiene un **Programma di Sviluppo** dei sistemi Informativi nel quale tiene traccia della pianificazione e dello stato di avanzamento dei progetti di sviluppo evolutivo dei sistemi informativi e della loro piattaforma tecnologica e applicativa.

4.2.2 Descrizione dei contenuti

Il **RSSI** adotta il formato e le modalità per lui più agevoli ed efficaci per compilare e gestire la documentazione del Programma degli Interventi, come ad esempio **cartelle EXCEL**, con tutta la documentazione allegata, descrittiva della storia degli interventi pianificati ed effettuati.

E' opportuno che gli interventi tracciati siano sintetizzati in forma tabellare, riportando per ciascun intervento almeno le seguenti informazioni:

ID	Titolo	Tipo	Data Target	Stato	Incaricato	Annotazioni

In cui:

- **ID**: è un identificativo univoco dell'intervento pianificato;
- **Titolo**: è il titolo descrittivo dell'intervento che consente di inquadrarlo;
- **Tipo**: individua una o più delle seguenti categorie:
  - **HW:** modifica evolutiva della configurazione hardware dei sistemi e degli apparati
  - **OS**: modifica evolutiva della piattaforma tecnologica ICT (sistema operativo e altre componenti di base)
  - **AP**: modifica evolutiva del software applicativo del sottosistema informativo
  - **LG:** modifica evolutiva dell'ambiente logistico dove sono situati i sistemi e gli apparati informatici (locali e impianti di supporto)
  - **XX:** modifica non classificabile in nessuna nelle precedenti categorie.
- **Data Target:** data di riferimento per il completamento dell'intervento pianificato
- **Stato:** indica uno dei seguenti stati:
  - **Pr:** l'intervento è previsto in linea di massima ma non ancora pianificato: la data target è solo indicativa.
  - **Pi:**: l'intervento è definito e pianificato: la data target è significativa ma può ancora subire qualche aggiustamento.
  - **Es**: l'intervento è in esecuzione: la data target è ormai consolidata e deve essere rispettata, salvo imprevisti gravi
  - **So:** l'intervento è stato sospeso: la data target non ha più significato o è solo indicativa per un'eventuale ripianificazione dell'intervento
  - **Co:** l'intervento è stato concluso: la data target indica la data di effettivo completamento delle attività
  - **XX:** l'intervento è stato cancellato: rimane solo traccia della sua storia.

- **Incaricato:** individua l'**IGSI** ossia la persona di riferimento, che è stata incaricata di eseguire o di controllare la corretta esecuzione dell'intervento, per assicurare che siano adottate le misure di sicurezza e garanzia previste in questi casi.
- **Annotazioni:** serve per fornisce ulteriori indicazioni utili e riferimenti ad eventuali altri documenti che illustrino le motivazioni, le peculiarità e i dettagli dell'intervento.

4.2.3 Gestione del documento

Il programma è redatto, pubblicato e gestito dal **RSSI**.

4.3 Registro di Gestione Configurazione

4.3.1 Scopo

L'obiettivo è tener traccia e documentare la storia di tutti gli interventi effettuati che hanno riguardato la configurazione della piattaforma tecnologica e l'ambiente logistico del sottosistema informativo; come ad esempio:

- la messa in esercizio delle modifiche evolutive pianificate nel "Programma do Sviluppo";
- l'installazione di nuovi componenti o nuove versioni del software di base e di supporto;
- l'applicazione di patch al software di base e al software applicativo;
- la sostituzione o la riparazione di componenti hardware o di parti degli stessi, che sono risultate guaste;
- il recupero e il ripristino dei dati danneggiati; ecc.

In sintesi, l'obiettivo è di tracciare tutti gli interventi riconducibili alla gestione straordinaria del sottosistema informativo.

4.3.2 Descrizione dei contenuti

Il formato del documento non è vincolante, purché contenga le informazioni richieste e sia mantenuto sempre aggiornato e rifletta correttamente la situazione corrente del sottosistema informativo.

Ad esempio si può utilizzare una struttura di **cartella EXCEL annuale** e tutta la documentazione allegata degli interventi effettuati.

E' necessario che il documento riporti per ciascun intervento effettuato almeno le seguenti informazioni:

Prot.	Data Rif.	Intervento	Tipo	Durata	Effettuato da	Verificato da	Cert	Annotazioni

In cui:

- **Prot:** è un numero di protocollo progressivo nell'anno (es. 06-125) dell'intervento eseguito;
- **Data Rif.**: è la data di riferimento di completamento dell'intervento e di messa in esercizio delle modifiche effettuate.

- **Intervento**: è il titolo descrittivo dell'intervento che consente di inquadrarlo;
- **Tipo**: individua una o più delle seguenti categorie:
  - **HW:** intervento sulla configurazione hardware dei sistemi e degli apparati
  - **OS**: intervento sulla piattaforma tecnologica ICT (sistema operativo e altre componenti di base)
  - **AP**: intervento sul software applicativo del sottosistema informativo
  - **LG:** intervento sugli apparati e gli impianti dell'ambiente logistico dove sono situati i sistemi e gli apparati informatici (locali e impianti di supporto)
  - **DA:** intervento di recupero e ripristino dei dati a seguito di un evento che ne aveva causato la distruzione o la perdita
  - **XX:** intervento non classificabile in nessuna nelle precedenti categorie.
- **Durata:** durata in ore dell'intervento per applicare e collaudare le modifiche sul sottosistema informativo in produzione. Nota: l'intervento potrebbe aver comportato la temporanea indisponibilità del servizio agli utenti.
- **Effettuato da:** identifica l'**IGSI** (interno o esterno) che ha materialmente eseguito l'intervento
- **Verificato da:** identifica l'**IGSI** (interno) che ha verificato la corretta esecuzione dei lavori e ha assicurato l'adozione delle misure di sicurezza e di garanzia applicabili in questi casi.
- **Cert:** indica (SI/NO/NA) se è stata fornita la certificazione di conformità che l'intervento non influisce negativamente sulla sicurezza del sottosistema informativo.
- **Annotazioni:** serve per fornisce ulteriori dettagli e indicazioni utili sull'intervento e i riferimenti all'eventuale documentazione di certificazione e di rendiconto dell'intervento.

4.3.3 Gestione del documento

Il registro deve essere aggiornato dagli **IGSI** ogni volta che viene effettuato un intervento.

Almeno una volta al mese, una copia elettronica deve essere inviata al **RSSI,** perché sia sempre aggiornato sugli sviluppi in corso e archivi l'edizione consolidata del documento.

4.4 Giornale di Gestione Applicazione

4.4.1 Scopo

L'obiettivo in questo caso è di documentare l'esecuzione delle procedure di gestione operativa ordinaria del sottosistema informativo; come ad esempio:

- l'attivazione, la disattivazione e la ripartenza del servizio quando ciò si rende necessario;
- l'esecuzione di procedure di switch-over e di switch-back per attivare le configurazioni d'emergenza in caso di necessità e per ripristinare la configurazione ordinaria quando è possibile il ritorno alla normalità

- l'esecuzione e la verifica delle procedure di acquisizione di dati da fonti esterne o di trasmissione dati verso sistemi esterni, secondo la programmazione prevista;
- l'esecuzione delle procedure periodiche di amministrazione dei dati;
- l'esecuzione e la verifica delle procedure di backup e di vaulting dei dati secondo la programmazione prevista;
- l'esecuzione di procedure di amministrazione degli utenti;
- la registrazione di eventuali problemi e non conformità riscontrate nel normale operatività del sistema;
- le azioni correttive intraprese e le segnalazioni effettuate;
- il recupero e il ripristino dei dati dai supporti di backup.

4.4.2 Descrizione dei contenuti

Il formato del documento non è vincolante, purché contenga le informazioni richieste e sia mantenuto sempre aggiornato e rifletta correttamente la situazione corrente del sottosistema informativo.

Ad esempio si può utilizzare una struttura di **cartella EXCEL annuale** e tutta la documentazione allegata degli interventi effettuati.

E' necessario che il documento riporti per ciascun Evento/Intervento almeno le seguenti informazioni:

Seq.	Data/Ora	Evento/Intervento	Tipo	Effettuato da	Annotazioni

In cui:

- **Seq.:**: è un numero progressivo nell'ambito del periodo di riferimento del Giornale di Gestione
- **Data/Ora**: è la data/ora di riferimento dell'evento o di completamento dell'intervento operativo eseguito
- **Evento/Intervento**: è il titolo descrittivo dell'evento/intervento che consente di inquadrarlo;
- **Tipo**: individua una delle seguenti categorie:
  - **Pb:** è stato rilevato un problema che deve essere gestito
  - **Ac:** è stata intrapresa un'azione correttiva a fronte di un problema riscontrato
  - **Op:** è stata effettuata un'operazione di ordinaria di gestione operativa dell'applicazione, come ad esempio l'esecuzione di procedure amministrative dell'applicazione e dei dati occasionali o periodiche e di produzione di report
  - **Bk**: è stata eseguita una procedura ordinaria di Backup o di Vaulting dei dati
  - **Ck**. è stata eseguita una procedura ordinaria di verifica della corretta funzionalità del sottosistema informativo
  - **XX:** intervento operativo non classificabile in nessuna nelle precedenti categorie.
- **Effettuato da:** identifica l'**IGSI** (interno o esterno) che ha materialmente eseguito l'intervento

- **Annotazioni:** serve per fornisce ulteriori dettagli e indicazioni utili sull'intervento e i riferimenti all'eventuale documentazione di supporto e di rendiconto dell'intervento.

4.4.3 Gestione del documento

Il documento è amministrato dagli **IGSI.** Per ogni periodo stabilito (i.e. mese, settimana o giornata) viene aperto un nuovo Giornale di Gestione.

Il Giornale di Gestione Applicazione corrente deve essere aggiornato e salvato dagli **IGSI** su una cartella condivisa e al termine di ogni turno deve esserne salvata anche una copia di backup.su un supporto rimovibile (es. memory stick) per poterlo riprendere in caso di necessità.

Al termine del periodo stabilito, Il Giornale di Gestione viene chiuso e deve esserne inviata una copia elettronica al **RSSI,** perché ne prenda atto ed archivi il documento tra gli atti del sottosistema informativo censito.

4.5 Certificazione dell'intervento

4.5.1 Scopo

Quando il **RSSI** si avvale di soggetti esterni (fornitore) per adottare nuove misure di sicurezza o per potenziarle, deve richiedere all'installatore una descrizione scritta dell'intervento effettuato che ne **attesta la conformità alle disposizioni del disciplinare tecnico(Allegato B del DLgs. 196/03)**.

La certificazione è necessaria per tutti gli interventi che modificano o possono violare le misure di sicurezza del sottosistema informativo, della sua piattaforma tecnologica o del suo ambiente logistico; come ad esempio, ma non solo:

- l'installazione di sistemi di video sorveglianza, di controllo degli accessi e antiintruzione;
- la configurazione dell'infrastruttura ICT e degli strumenti di sicurezza logica (firewall, IDS e antivirus);
- l'installazione e la configurazione di sistemi di gestione delle credenziali per l'autenticazione e l'autorizzazione degli utenti del sottosistema informativo;
- l'esecuzione di interventi di hardening dei sistemi della piattaforma tecnologica;
- la distruzione o il recupero di supporti fisici contenenti dati sensibili.

4.5.2 Descrizione dei contenuti

Si tratta di un normale rapporto di regolare esecuzione dei lavori, per il quale non è prescritto un particolare formato, i cui contenuti devono essere tali da descrivere chiaramente la natura dell'intervento effettuato; ma deve riportare chiaramente la seguente attestazione di conformità:

"Il fornitore attesta che il risultato dell'intervento è conforme alle disposizioni ricevute dall'ASL e a quelle del disciplinare tecnico (Allegato B del DLgs 196/03)."

4.5.3 Gestione del documento

Il documento deve essere predisposto dal fornitore, sottoscritto dal **RE** del fornitore e consegnato al **RSSI** o ad un suo incaricato, alla conclusione dell'intervento.

L'avvenuta certificazione dell'intervento deve essere annotata nella voce corrispondente del **Giornale di Gestione Configurazione** e il documento deve essere messo agli atti del sottosistema informativo

5 Compilazione del Libretto di Sistema

Lo scopo di questa parte delle Linee Guida è di fornire maggiori spiegazioni per una corretta compilazione del Libretto di Sistema, affinché diventi un utile strumento di supporto per la corretta gestione dei Sistemi Informativi. Si noterà che i capitoli che seguono riflettono la struttura del Libretto di Sistema per fornire le indicazioni e le spiegazioni opportune.

Intestazione del Libretto di Sistema

Lo scopo di questa sezione del Libretto di Sistema e di identificare univocamente il sottosistema informativo nel quadro generale definito da **SSI** nel documento *"Analisi dello stato delle risorse ICT - Piano triennale di sviluppo 2006-2008",* utilizzando la stessa tassonomia e la stessa codifica.

Per comodità si riportano di seguito le aree di pertinenza in cui si collocano i sottosistemi informativi aziendali:

- **Servizi Infrastrutturali**: servizi abilitanti che costituiscono l'ossatura informatica e di connettività di base del sottosistema informativo e ne permettono la gestione secondo parametri di efficienza e sicurezza (networking, desk top management, security perimetrale ed interna, etc.);
- **Servizi Trasversali:** servizi comuni e condivisi di tipo comunicativo e di automazione d'ufficio, che forniscono il necessario supporto alle attività produttive dei gruppi di lavoro aziendali e alle relazioni esterne ed interne (posta elettronica, portale aziendale, intranet, etc.);
- **Servizi Territoriali:** servizi applicativi, sia di tipo amministrativo, sia di tipo assistenziale, destinati a fornire supporto alle attività di prevenzione ed assistenziali post-acute, proiettate quindi verso le aree territoriali di competenza dell'azienda (p.es.: rete di relazioni con i MMG-PLS, farmaceutica territoriale, ADI, Anagrafe Assistibili, etc.);
- **Servizi Clinico-Ospedalieri:** servizi applicativi destinati a fornire supporto alle attività di tipo specialistico ambulatoriale ed ospedaliero, con la gestione dei sistemi di cura e dei sistemi amministrativi correlati (p.es.: Sistema Informativo Integrato Ospedaliero, Laboratorio Analisi. RIS-PACS, etc.)
- **Servizi Amministrativi:** servizi applicativi che sono finalizzati alla gestione operativa delle attività amministrative centrali dell'azienda sanitaria, con particolare riferimento alla gestione economico-patrimoniale ed alla gestione delle risorse umane;
- **Servizi Direzionali:** servizi applicativi che forniscono strumenti di controllo e monitoraggio direzionale in relazione agli indicatori di natura epidemiologica e produttiva che caratterizzano il dimensionamento dei consumi e delle prestazioni aziendali, e che permettono di analizzare e supportare le decisioni di orientamento delle risorse disponibili.

Nell'intestazione del Libretto di Sistema vanno riportate le seguenti informazioni:

- **Area** – indica l'area di pertinenza del sottosistema informativo censito e documentato

- **Sistema** – è la denominazione del sistema aziendale di riferimento al quale appartiene il sottosistema informativo censito e documentato
- **Sottosistema** – è la denominazione del sottosistema informativo censito e documentato
- **Codice** – è una sigla breve che individua univocamente il sottosistema codice
- **Contesto** – classifica il contesto di riferimento nel quale si colloca il sottosistema informativo censito e la sua valenza. Può assumere i seguenti valori:
  - Locale
  - Aziendale
  - Regionale
  - Nazionale
  - Internazionale
- **Titolare Sistema** – è l'unità organizzativa titolare del sottosistema informativo
- **Responsabile Gestione** – è l'unità organizzativa responsabile della gestione del sottosistema informativo
- **Rif. Normativi -** riporta gli eventuali riferimenti normativi che giustificano il sottosistema informativo

Sezione A - Finalità del Sottosistema Informativo e Organizzazione di Supporto

Lo scopo di questa sezione è di sintetizzare le informazioni qualificanti ai fini della privacy, ossia:

- la funzione del sottosistema informativo, ossia i tipi di attività che supporta
- gli utenti che lo utilizzano
- il genere di dati personali che vengono trattati
- gli interessati dei dati personali trattati
- gli altri sistemi con cui si interfaccia o interagisce
- la ripartizione delle responsabilità per la sua gestione e il suo supporto

Il modello è autoesplicativo.

Sezione B - Architettura e Logistica della Piattaforma Tecnologica

Lo scopo di questa sezione è di sintetizzare le caratteristiche fondamentali della piattaforma tecnologica utilizzata in modo da avere un quadro generale delle sue caratteristiche, della sua affidabilità e della sua sicurezza, per poterne ricavare utili elementi per:

- supportare e ottimizzare la gestione dei sottosistemi informativi aziendali;
- razionalizzare e ottimizzare l'evoluzione, abilitando e facilitando il processo di consolidamento e standardizzazione delle infrastrutture ICT, delle piattaforme tecnologiche e di integrazione dei sistemi informativi, che sono alla base del già citato Piano Triennale di evoluzione dei Sistemi Informativi.

In questo ambito si dovranno evidenziare le peculiarità e le caratteristiche salienti di affidabilità e sicurezza di:

- architettura della piattaforma tecnologica;
- ubicazione dei sistemi e degli apparati;
- collocazione delle stazioni di lavoro;
- custodia dei documenti dei supporti rimovibili del sottosistema informativo.

Il modello è autoesplicativo.

Sezione C - Politiche di Gestione del Servizio

Questa sezione sintetizza gli elementi qualificanti della gestione operativa del sottosistema informativo evidenziando le politiche adottate per:

- Amministrazione degli utenti;
- Integrazione con altri sistemi;
- Backup e il Vaulting dei dati;
- Aggiornamento del Software di Sistema;
- Aggiornamento del Software Applicativo;
- Disaster Recovery.

Il modello è autoesplicativo

Sezione D - Livello di Servizio garantito

Lo scopo di questa sezione è di sintetizzare le caratteristiche del servizio garantito fornendo degli indicatori misurabili.

Di seguito si riportano i parametri e gli indicatori richiesti con degli esempi di come possono essere impostati.

Orari di riferimento

Possono essere definiti più orari di riferimento da richiamare nella definizione degli indicatori del Livello di Servizio.

Orario	**Definizione**	
Orario Ordinario	Lunedì a Venerdì Sabato e prefestivi Domenica e Festivi	Dalle 09:00 alle 18:00 Dalle 09:00 alle 12:00 Non Applicabile
Orario Esteso	Lunedì a Venerdì Sabato e prefestivi Domenica e Festivi	Dalle 08:00 alle 20:00 Dalle 09:00 alle 12:00 Non Applicabile
Orario Continuato	24/24h 6/7g 50/52s	

Tabella 1- esempio di orari di riferimento

Disponibilità del servizio

Esprime in percentuale il tempo effettivo di disponibilità del Servizio durante l'orario di riferimento durante il periodo di osservazione

Orario di Riferimento	Orario Esteso
Periodo di Osservazione	Trimestrale
Disponibilità	>99,5%

Tabella 2 - esempio di disponibilità del servizio

Risposta ordinaria alle chiamate

La presa in carico della chiamata comporta l'esecuzione delle procedure di ripristino del servizio (anche se solo in modalità di emergenza), la diagnosi del problema e eventualmente l'attivazione della manutenzione correttiva per la risoluzione definitiva del problema.

Orario di Riferimento	Orario Ordinario
Periodo di Osservazione	Trimestrale
Presa in Carico	< 30' nel 99,0% dei casi
Ripristino Operatività	< 1h nel 99% dei casi

Tabella 3 - esempio di risposta ordinaria alle chiamate

Risposta alle chiamate fuori orario

La presa in carico della chiamata comporta l'esecuzione delle procedure di ripristino del servizio (anche se solo in modalità di emergenza), la diagnosi del problema e eventualmente l'attivazione della manutenzione correttiva per la risoluzione definitiva del problema

Orario di Riferimento	Orario Continuato
Periodo di Osservazione	Trimestrale
Presa in Carico	< 4h nel 90,0% dei casi
Ripristino Operatività	< 1h nel 90% dei casi
Reperibilità	24/24h 365/365g

Tabella 4 - esempio di risposta alle chiamate fuori orario

Fix del software

Il **Fix** definitivo del software viene effettuato dopo che il problema è stato diagnosticato e il servizio è stato ripristinato (anche se in modalità di emergenza)

Orario di Riferimento	Orario Ordinario
Periodo di Osservazione	Semestrale

Tabella 5 - esempio di fix del software

La manutenzione del software deve essere completata in base alla severità del problema secondo prospetto seguente:

Sev.	Tempo	Note
1	< 8h nel 90% dei casi	Per problemi che causano l'indisponibilità totale del servizio on-line o di sue componenti critiche per la corretta operatività degli utenti del sottosistema informativo Per problemi che impattano la corretta esecuzione di procedure batch da completare in finestre temporali strette per interfacciare altri sistemi
2	< 48h nel 90% dei casi	Per problemi che impattano la normale operatività delle procedure batch automatiche o di quelle manuali eseguite gioenalemente o in occasioni di scadenze predefinite con finestre temporali strette.
3	< 5g nel 90% dei casi	Per problemi che impattano marginalmente le funzionalità del sottosistema informativo

Tabella 6 - esempio di parametrizzazione in base alla severità

In ogni caso il **backlog** delle **Fix** da sviluppare non deve mai superare i 10 gg lavorativi.

Manutenzione HW

Gli interventi di manutenzione del hw devono essere effettuati on-site secondo il seguente prospetto.

L'intervento prevede la diagnosi del problema, l'attivazione delle risorse d'emergenza, l'individuazione della parte da sostituire e la sua sostituzione se disponibile a magazzino, altrimenti va attivata l'acquisizione all'esterno del pezzo di ricambio e quindi l'installazione dello stesso quando è finalmente disponibile

Modalità	Note
95% < 4h in giornata	Se la chiamata viene effettuata entro le 16:00 dei giorni feriali e entro le ore 12:00 del sabato e dei prefestivi
95% < 4h del primo giorno lavorativo	Se la chiamata vene effettuata dopo le ore 16: dei giorni feriali o dopo le ore 12:00 del sabato e dei prefestivi
90% < 8h nei giorni festivi	Per le sole emergenze che rendono totalmente indisponibile il sistema
1 al trimestre	Manutenzione preventiva dei sistemi

Tabella 7 - esempio di parametrizzazione della manutenzione hw

Sezione E - Attestazione di Conformità delle Misure di Sicurezza

In questa sezione il RGSI attesta la conformità del sottosistema informativo e della sua gestione alle disposizioni di Legge che riguardano le misure minime di sicurezza (Allegato B DLgs 196/03).

Il modello è autoesplicativo