Libretto di Sistema

|  |  |  |  |
| --- | --- | --- | --- |
| **ASSL[[1]](#footnote-1)** |  | **Area[[2]](#footnote-2)** |  |
| **Sottosistema[[3]](#footnote-3)** |  | **Codice** |  |
| **Contesto[[4]](#footnote-4)** |  | **Titolare Sistema[[5]](#footnote-5)** |  |
| **Responsabile**  **Gestione[[6]](#footnote-6)** |  | **Data Agg.[[7]](#footnote-7)** |  |

Riferimenti Normativi

|  |
| --- |
|  |

Note

|  |
| --- |
|  |

[Sezione A Libretto di Sistema in Specificazione dei Requisiti del PMA 3](#_Toc178173679)

[Sezione B Finalità del Sistema Informativo e Organizzazione di Supporto 5](#_Toc178173680)

[B.1 Funzione del sistema informativo e caratteristiche dei trattamenti effettuati 5](#_Toc178173681)

[B.1.1 Descrizione sintetica del/dei trattamento/i attuato/i 5](#_Toc178173682)

[B.1.2 Definizione sintetica della finalità del/dei trattamento/i 5](#_Toc178173683)

[B.1.3 Elencazione sintetica dei processi di trattamento 5](#_Toc178173684)

[B.1.4 Indicazione della categoria del/dei trattamento/i 5](#_Toc178173685)

[B.1.5 Indicazione delle categorie di dati personali trattati 5](#_Toc178173686)

[B.1.6 Indicazione delle categorie di soggetti interessati al/ai trattamento/i 5](#_Toc178173687)

[B.1.7 Registrazione del trattamento nel Registro dei Trattamenti 5](#_Toc178173688)

[B.2 Utenti che lo utilizzano 5](#_Toc178173689)

[B.3 Altri sistemi con cui si interfaccia o interagisce 6](#_Toc178173690)

[B.4 Ripartizione delle responsabilità per la sua gestione e il suo supporto 6](#_Toc178173691)

[Sezione C Architettura e Logistica della piattaforma tecnologica 7](#_Toc178173692)

[C.1 Architettura della piattaforma tecnologica 7](#_Toc178173693)

[C.2 Ubicazione dei sistemi e degli apparati 7](#_Toc178173694)

[C.3 Collocazione delle stazioni di lavoro 7](#_Toc178173695)

[C.4 Custodia dei supporti rimovibili del sistema informativo 7](#_Toc178173696)

[Sezione D Politiche di Gestione del Servizio 8](#_Toc178173697)

[D.1 Amministrazione degli utenti 8](#_Toc178173698)

[D.2 Integrazione con altri sistemi 8](#_Toc178173699)

[D.3 Backup e Vaulting dei dati 8](#_Toc178173700)

[D.4 Aggiornamento del Software di Sistema 8](#_Toc178173701)

[D.5 Aggiornamento del Software Applicativo 8](#_Toc178173702)

[D.6 Disaster Recovery 8](#_Toc178173703)

[Sezione E Livello di Servizio garantito 9](#_Toc178173704)

[E.1 Orari di Riferimento (R7) 9](#_Toc178173705)

[E.2 Disponibilità del Servizio (R8) 9](#_Toc178173706)

[E.3 Modalità di Attivazione delle Chiamate (R9) 9](#_Toc178173707)

[E.4 Tempi di Risposta Ordinaria alle Chiamate di Assistenza Applicativa (R10) 9](#_Toc178173708)

[E.5 Tempi di Risposta alle Chiamate Fuori Orario di Assistenza Applicativa (R11) 11](#_Toc178173709)

[E.6 Fix del Software (R12) 11](#_Toc178173710)

[E.7 Tempi di Risposta alle Chiamate di Manutenzione Hardware (R13) 12](#_Toc178173711)

[Sezione F Attestazione di conformità delle misure di sicurezza 13](#_Toc178173712)

[F.1 Trattamenti che comportano la notifica al Garante 13](#_Toc178173713)

[F.2 Indicazione del livello di rischio valutato 13](#_Toc178173714)

[F.3 Misure di sicurezza adottate 13](#_Toc178173715)

[F.3.1 Autenticazione informatica degli utenti (Incaricati dei trattamenti) 13](#_Toc178173716)

[F.3.2 Procedure di gestione delle credenziali degli incaricati dei trattamenti 13](#_Toc178173717)

[F.3.3 Sistema di autorizzazione degli accessi 13](#_Toc178173718)

[F.3.4 Aggiornamento periodico dei profili di autorizzazione degli Incaricati 13](#_Toc178173719)

[F.3.5 Protezione degli strumenti elettronici e dei dati 13](#_Toc178173720)

[F.3.6 Copie di sicurezza dei dati 13](#_Toc178173721)

[F.3.7 Pseudonimizzazione e cifratura dei dati sensibili 13](#_Toc178173722)

[F.3.8 Misure di tutela e garanzia 14](#_Toc178173723)

[F.3.9 Ulteriori misure di sicurezza 14](#_Toc178173724)

[F.3.10 Adeguatezza delle misure di sicurezza 14](#_Toc178173725)

# Libretto di Sistema in Specificazione dei Requisiti del PMA

Si riportano di seguito i riferimenti applicabili alle Specifiche dei Requisiti del PMA:

* + **(R1.2)** L’Azienda Fornitrice del servizio, come conseguenza della nomina in qualità di ***Responsabile del Trattamento dei Dati Personali***, dovrà produrre entro 40 (quaranta) giorni lavorativi dalla sottoscrizione del contratto adeguata documentazione, integrando il relativo **Libretto di Sistema**, che contenga almeno:
  + L’elenco dei sottosistemi di propria pertinenza che svolgono operazioni di trattamento dei dati personali e/o sensibili, con la specificazione, in riferimento ad essi, di:
    1. descrizione sintetica del/dei trattamento/i attuato/i;
    2. definizione sintetica della finalità del/dei trattamento/i;
    3. elencazione sintetica dei processi di trattamento;
    4. indicazione della categoria del/dei trattamento/i;
    5. indicazione delle categorie di dati personali trattati;
    6. indicazione delle categorie di soggetti interessati al/ai trattamento/i;
    7. riferimento al/ai trattamenti per come tracciato nel Registro dei Trattamenti.
  + Indicazione del livello di rischio valutato *ex-ante* in relazione al/ai trattamento/i attuato/i con i propri sottosistemi.
  + Indicazione delle correlate misure di sicurezza di natura tecnica e organizzativa, già adottate e/o che si intendono comunque adottare nell’arco del periodo contrattuale (non oltre il primo anno di validità contrattuale nel caso di contratti pluriennali), per limitare il rischio di violazione o perdita dei dati personali e/o sensibili oggetto del trattamento; a titolo esemplificativo - e comunque non esaustivo - le misure di sicurezza di natura tecnica (informatica) che dovranno essere garantite sono quelle previste dal paragrafo 4 dell’articolo 28 del Regolamento Europeo 2016/679, ovvero (citazione dal GDPR):
    1. *la pseudonimizzazione e la cifratura dei dati personali;*
    2. *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
    3. *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
    4. *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

e/o anche quelle previste dalla Circolare ANAC 18/04/2017 n. 2/2017 relative alle Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni.

* ***(R1.5.1) Libretti di Sistema*** per ciascun sottosistema, da inviare entro 40 (quaranta) giorni lavorativi dalla sottoscrizione del contratto, con comunicazione scritta ad ARES, effettuata a mezzo di PEC agli indirizzi che verranno successivamente comunicati. Ciascun Libretto sarà compilato secondo quanto indicato nel modello del Libretto di Sistema 2020-2022. Il relativo file dovrà essere denominato, in alternativa, come segue:
  + *<ARES><codice sottosistema>\_LibrettoSistema\_<aaaa>*;
  + *<ASSL><NUM(1)><codice sottosistema>\_LibrettoSistema\_<aaaa>*;

dove *<ASSL><NUM(1)>* rappresenta la ASSL di riferimento

*e <aaaa>* rappresenta l’anno di riferimento.

Si precisa che in caso di contratti con durate superiori ad un anno, i Libretti di Sistema dovranno essere emessi almeno annualmente, e comunque a seguito di variazioni significative delle configurazioni o a seguito dell’esito di eventuali attività ispettive condotte da ARES.

Il Fornitore rilascerà inoltre, come allegato al Libretto di Sistema, una dettagliata documentazione tecnica a riguardo della descrizione dell'architettura del sistema, dell'ambiente applicativo (con particolare riferimento ai moduli di integrazione e ai relativi flussi di informazioni), delle procedure di manutenzione ordinaria e straordinaria dei sistemi (inclusi i test di verifica disponibilità dei servizi e le procedure operative di primo intervento) e, ove possibile, dell’organizzazione nonché della struttura fisica e logica dei database, delle correlazioni tra tabelle e tra moduli applicativi.

Il Fornitore si impegna, in caso di variazioni sui sistemi, ad aggiornare tempestivamente la suddetta documentazione (incluso il Libretto di Sistema) ed a ritrasmetterla ad ARES, sempre a mezzo di PEC.

Il Fornitore è inoltre tenuto a dichiarare nel Libretto di Sistema, entro 40 (quaranta) giorni lavorativi dalla stipula del rapporto contrattuale (accettazione dell’ordinativo), l’adeguatezza delle Misure di Sicurezza che ha già adottato per la protezione dei dati personali e sensibili in funzione dei requisiti delle attività di servizio e alla relativa classificazione di livello di criticità del sottosistema informativo oggetto dello stesso, e ad evidenziare con cadenza almeno trimestrale, con apposita comunicazione, la loro verifica periodica.

Il Libretto di Sistema è conservato da ARES all’interno del sistema di *accountability* aziendale, ai sensi dell’articolo 24, comma 1 del Regolamento Europeo 2016/679.

# Finalità del Sistema Informativo e Organizzazione di Supporto

## Funzione del sistema informativo e caratteristiche dei trattamenti effettuati

Indicare il contesto operativo in cui si colloca il sistema e le attività svolte per mezzo del sistema stesso.

### Descrizione sintetica del/dei trattamento/i attuato/i

Elencare sinteticamente i trattamenti effettuati facendo uso del sistema informativo (es. trattamento dei dati dei dipendenti; trattamento dei dati di contatto dei fornitori). Per trattamento si intende qualsiasi operazione o insieme di operazioni, compiute con l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali

### Definizione sintetica della finalità del/dei trattamento/i

Indicare le finalità dei trattamenti effettuati facendo ricorso al sistema informativi (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini). Sarebbe opportuno indicare anche la base giuridica del trattamento.

### Elencazione sintetica dei processi di trattamento

Indicare sinteticamente, per ciascun trattamento individuato, i processi che vengono svolti (p.es. la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione, etc.)

### Indicazione della categoria del/dei trattamento/i

Con riferimento alla “descrizione delle categorie di trattamenti effettuati” (art. 30, par. 2, lett. b) del RGPD) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell’art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest’ultimo

### Indicazione delle categorie di dati personali trattati

"Dato personale": qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; (v. ex-D.lgs 196/2003, Art. 4). Es: dati anagrafici, dati clinici, dati sanitari, dati contabili ecc Andranno specificate le categorie di dati personali oggetto di ogni trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.)

### Indicazione delle categorie di soggetti interessati al/ai trattamento/i

Iinteressati": le persone fisiche, le persone giuridiche, gli enti o le associazioni cui si riferiscono i dati personali (v. ex-D.lgs 196/2003, Art. 4). Andranno specificate le tipologie di soggetti interessati (es. clienti, fornitori, dipendenti, cittadini, pazienti, etc.)

### Registrazione del trattamento nel Registro dei Trattamenti

Andranno specificate le tipologie di soggetti interessati (es. clienti, fornitori, dipendenti, cittadini, pazienti, etc.)

## Utenti che lo utilizzano

Indicare il tipo di utenza (es. personale amministrativo, medico ecc.) ed eventualmente l’ufficio e/o il servizio di appartenenza.

## Altri sistemi con cui si interfaccia o interagisce

Indicare “nessuno”, se non applicabile. Indicare, se presenti, quali dati vengono movimentati da e verso altri sistemi e/o sono acceduti da altri sistemi.

## Ripartizione delle responsabilità per la sua gestione e il suo supporto

Indicare i soggetti coinvolti in gestione e supporto del sistema specificando le relative competenze/responsabilità con riferimento anche alle specifiche contrattuali e ai requisiti sottoscritti nell’ambito del piano di assistenza e manutenzione annuale.

# Architettura e Logistica della piattaforma tecnologica

## Architettura della piattaforma tecnologica

Indicare per ogni apparato e sistema server coinvolto:

* marca, modello e numero seriale e dati di configurazione hardware rilevanti, inclusi eventuali componenti aggiuntivi
* configurazione di rete e hostname, anche per le eventuali macchine virtuali
* prodotti software di base e prodotti software applicativo installati completi di versione e indicazione di eventuali componenti specifici, anche per eventuali macchine virtuali

Riportare inoltre una chiara descrizione dell’architettura hardware e software e delle correlazioni e delle interazioni tra moduli applicativi, possibilmente accompagnate da una rappresentazione grafica esplicativa.

Indicare i requisiti minimi hardware e software delle postazioni client.

## Ubicazione dei sistemi e degli apparati

Indicare: indirizzo, piano, stanza-ufficio in cui sono collocati gli apparati che fanno parte del sistema.

## Collocazione delle stazioni di lavoro

Indicare indirizzo/i, piano, stanza-ufficio in cui sono collocate le postazioni per mezzo delle quali il sistema viene utilizzato e il numero - almeno indicativo - di postazioni attive per sede.

## Custodia dei supporti rimovibili del sistema informativo

Indicare le modalità di archiviazione e custodia dei supporti rimovibili e relativa responsabilità.

# Politiche di Gestione del Servizio

## Amministrazione degli utenti

Indicare:

* le procedure di assegnazione[[8]](#footnote-8), creazione e consegna delle credenziali di accesso al sistema delle utenze di accesso.
* le politiche di sicurezza adottate per la gestione delle password, inclusa l’implementazione sul sistema di vincoli di complessità e periodi di validità (scadenza) delle password.

## Integrazione con altri sistemi

Fare riferimento al punto A.5, se sono già state indicate le politiche di integrazione.

## Backup e Vaulting dei dati

Per ciascuna categoria di operazioni di backup effettuata sul sistema si richiede la compilazione, conformemente a quanto riportato in contratto, di una tabella che includa i seguenti campi:

|  |  |
| --- | --- |
| **Oggetto del backup** |  |
| **Modalità di backup** |  |
| **Periodicità** | *(almeno giornaliera)* |
| **Modalità di verifica** |  |

In caso di backup su supporto rimovibile indicare il tipo e il numero dei supporti rimovibili utilizzati per backup giornaliero, settimanale e mensile.

E’ gradito documento specifico (da allegare al presente libretto) che descriva in particolare le procedure di backup e vaulting (modalità, supporti e/o apparati utilizzati, periodicità, eventuale schedulazione in caso di operazioni automatizzate).

## Aggiornamento del Software di Sistema

Indicare livello di aggiornamento alla data di compilazione e periodicità/pianificazione degli aggiornamenti. Evidenziare eventuali criticità che impediscono l’aggiornamento del software di sistema.

## Aggiornamento del Software Applicativo

Indicare livello di aggiornamento alla data di compilazione e periodicità/pianificazione degli aggiornamenti. Evidenziare eventuali criticità che impediscono l’aggiornamento del software applicativo.

## Disaster Recovery

In caso di assenza di un ambiente di disaster recovery indicare la configurazione hardware minima di necessaria al ripristino temporaneo dei servizi (anche se con prestazioni ridotte).

# Livello di Servizio garantito

Ai fini della definizione dei Livelli di Servizio (SLA) le anomalie rilevabili sul sistema sono classificate secondo criteri di gravità ed urgenza come segue:

problema bloccante: investono l'ambiente operativo e le attività critiche del servizio aziendale interessato; l’operatività di una parte significativa degli utenti interni e/o esterni è altamente compromessa; sono bloccanti anche le anomalie che impattano sulla corretta esecuzione di procedure batch da completare in finestre temporali definite per interfacciare altri sistemi e consentirne l’uso.

problema grave: la normale attività degli utenti e/o l’erogazione di un servizio è fortemente degradata; sono gravi anche i problemi che impattano sulla normale operatività delle procedure batch automatiche o di quelle manuali eseguite giornalmente o in occasioni di scadenze predefinite con finestre temporali strette.

problema secondario: impatta marginalmente sull’operatività degli utenti interni ed esterni.

## Orari di Riferimento (R7)

Sono definiti “Orari di Riferimento” le finestre temporali in cui si richiede l’erogazione del servizio di assistenza e manutenzione da parte del Fornitore.

L’”Orario Ordinario” viene utilizzato come elemento di specificazione nella definizione degli SLA al paragrafo “Tempi di Risposta Ordinaria alle Chiamate di Assistenza Applicativa”. Ciascuno degli altri orari di riferimento eventualmente richiesto viene invece utilizzato come elemento di specificazione nella definizione degli SLA indicati al paragrafo “Tempi di Risposta alle Chiamate Fuori Orario di Assistenza Applicativa”.

Per ciascuna categoria di orario di riferimento previsto, si richiede di compilare la seguente tabella conformemente a quella già riportata in contratto.

| **Orario** | **Definizione** |
| --- | --- |
| Orario Ordinario (R7.1) |  |
| Orario Esteso (R7.2) |  |
| Orario Festivo (R7.3) |  |

## Disponibilità del Servizio (R8)

Questa misura esprime in percentuale il tempo effettivo di disponibilità del Servizio/ Sottosistema nell’orario di riferimento, durante il periodo di misurazione.

Si richiede di compilare la seguente tabella conformemente a quella già riportata in contratto.

|  |  |
| --- | --- |
| **Orario di Riferimento** | Orario Ordinario + Orario Esteso (se previsto) + Orario Festivo (se previsto) |
| **Periodo di Misurazione** | Trimestrale, Semestrale, Annuale |
| **Disponibilità** |  |

## Modalità di Attivazione delle Chiamate (R9)

Le modalità di segnalazione di blocchi o anomalie di sistema devono essere indicate secondo il prospetto seguente. Si richiede pertanto di compilare una tabella contenente i seguenti campi conformemente a quella già riportata in contratto:

|  |  |  |
| --- | --- | --- |
| **Orario** | **Modalità** | **Dettagli** |
| Periodo Settimanale:  Orario: | Telefono | *<numero telefonico>* |
| … | … | … |

## Tempi di Risposta Ordinaria alle Chiamate di Assistenza Applicativa (R10)

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 (in ogni caso dovrà essere rispettata la procedura di cui al capitolo 3 delle Specifiche Contrattuali).

Si riportano di seguito le caratteristiche dei tempi di risposta ordinaria alle chiamate in funzione della criticità dei sottosistemi come da Specifiche Contrattuali. Si richiede pertanto di riportare la tabella (tra le seguenti) applicabile nel contesto del sottosistema in oggetto, conformemente quanto contrattualmente previsto.

Tempi di Risposta richiesti per Sistemi con **criticità alta**

|  |  |  |  |
| --- | --- | --- | --- |
| **Orario di Riferimento** | Ordinario | | |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di Presa in Carico** | 1 ora | 2 ore | 2 gg lavorativi |
| **Tempo di ripristino operatività dalla presa in carico** | 2 ore | 4 ore | 4 gg lavorativi |
| **Livelli di Servizio** | Il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **99%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **90%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nell’ **80%** dei casi. |

Tempi di Risposta richiesti per Sistemi con **criticità media**

|  |  |  |  |
| --- | --- | --- | --- |
| **Orario di Riferimento** | Ordinario | | |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di Presa in Carico** | 2 ore | 4 ore | 4 gg lavorativi |
| **Tempo di ripristino operatività dalla presa in carico** | 4 ore | 8 ore | 6 gg lavorativi |
| **Livelli di Servizio** | Il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **99%** dei casi | Il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **90%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nell’ **80%** dei casi. |

Tempi di Risposta richiesti per Sistemi con **criticità bassa**

|  |  |  |  |
| --- | --- | --- | --- |
| **Orario di Riferimento** | Ordinario | | |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di Presa in Carico** | 4 ore | 8 ore | 6 gg lavorativi |
| **Tempo di ripristino operatività dalla presa in carico** | 8 ore | 2 gg lavorativi | 12 gg lavorativi |
| **Livelli di Servizio** | Il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **99%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **90%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nell’ **80%** dei casi. |

## Tempi di Risposta alle Chiamate Fuori Orario di Assistenza Applicativa (R11)

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.

Qualora non sia prevista copertura contrattuale in orario non “ordinario” (“Esteso” e/o “Festivo”) indicare “servizio di assistenza fuori orario non previsto”, altrimenti riportare la tabella (tra le seguenti) applicabile nel contesto del contratto di manutenzione del sottosistema in oggetto.

Tempi di Risposta richiesti solo per Sistemi con **criticità alta**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Orario di Riferimento** | Esteso | | |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di Presa in Carico** | 2 ore | 4 ore | - |
| **Tempo di ripristino operatività dalla presa in carico** | 4 ore | 8 ore | - |
| **Livelli di Servizio** | Il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **99%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **90%** dei casi | - |

|  |  |  |  |
| --- | --- | --- | --- |
| **Orario di Riferimento** | Festivo (con reperibilità telefonica) | | |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di Presa in Carico** | 2 ore | 4 ore | - |
| **Tempo di ripristino operatività dalla presa in carico** | 8 ore | 16 ore | - |
| **Livelli di Servizio** | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **99%** dei casi | il tempo di intervento e il tempo di ripristino dovranno essere rispettati, nel periodo di osservazione, nel **90%** dei casi | - |

## Fix del Software (R12)

Il Fix definitivo del software applicativo dovrà essere effettuato dopo che il problema è stato diagnosticato e il servizio è stato ripristinato, anche se in modalità di emergenza. La manutenzione del software deve essere completata in base alla severità del problema secondo prospetto seguente:

|  |  |  |  |
| --- | --- | --- | --- |
| **Periodo di Osservazione** | Trimestrale | | |
| **Gravità** | ***Problema bloccante*** | ***problema grave*** | ***problema secondario*** |
| **Tempo di produzione del Fix definitivo** | 2 gg lavorativi | 5 gg lavorativi | 30 gg lavorativi |

In ogni caso il backlog delle Fix da sviluppare non deve mai superare i trenta giorni lavorativi. Gli aggiornamenti devono essere corredati di documentazione contenente l’elenco dettagliato delle modifiche operate ed eventuali integrazioni dei manuali d’uso.

Si richiede pertanto, ove previsto il requisito R12, l’indicazione della tabella di cui al precedente punto D4 e, se prevista l’assistenza fuori orario, D5.

## Tempi di Risposta alle Chiamate di Manutenzione Hardware (R13)

Nel caso sia richiesta la manutenzione dell’hardware, gli interventi prevedono 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.

Per i Livelli di Servizio richiesti (e per le relative penali applicabili) si intendono applicabili i riferimenti ai tempi di chiamata, presa in carico e ripristino dell’operatività indicati nei precedenti paragrafi.

Qualora la manutenzione hardware non sia contrattualmente prevista (requisito R13), indicare “servizio di assistenza hardware non previsto”.

# Attestazione di conformità delle misure di sicurezza

## Trattamenti che comportano la notifica al Garante

Indicare se la notifica non è necessaria

## Indicazione del livello di rischio valutato

Indicare il livello di rischio valutato, indicando anche la metodologia utilizzata

## Misure di sicurezza adottate

Andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’art. 32 del RGDP tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al Responsabile del trattamento, di concerto con il Titolare, la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l’Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

### Autenticazione informatica degli utenti (Incaricati dei trattamenti)

Indicare i meccanismi di autenticazione utilizzati

### Procedure di gestione delle credenziali degli incaricati dei trattamenti

Se le procedure sono già state opportunamente descritte al punto C.1 fare riferimento alla sezione C.

### Sistema di autorizzazione degli accessi

Indicare se/come sono delimitati gli ambiti d’azione degli incaricati in termini di accesso ai dati e relative elaborazioni (ad es. attraverso l’assegnazione di ruoli utente)

### Aggiornamento periodico dei profili di autorizzazione degli Incaricati

Indicare tempi e casi in cui i profili di autorizzazione vengono controllati e aggiornati in base alle indicazioni dei titolari dei trattamenti (es. periodo di mancato utilizzo, cessazione del rapporto di lavoro ecc.) precisando che il RSSI ha richiesto l’invio trimestrale delle utenze applicative inutilizzate da almeno 6 mesi.

### Protezione degli strumenti elettronici e dei dati

Indicare le misure di sicurezza adottate, oltre a backup e vaulting dei dati, a prevenzione dei “rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta” (ad es. con riferimento alle misure di sicurezza fisica). Precisare in particolare la periodicità di verifica del corretto aggiornamento del software antivirus.

### Copie di sicurezza dei dati

Indicare come/dove vengono custodite le copie di sicurezza se non già riportato nelle sezioni precededenti.

### Pseudonimizzazione e cifratura dei dati sensibili

Indicare se/come i dati sensibili sono pseudonimizzati e/o cifrati, “nessuna” se non effettuata

### Misure di tutela e garanzia

Il fornitore si impegna a garantire la conformità alle precedenti misure di sicurezza anche a seguito di interventi di manutenzione ordinaria e straordinaria sul sistema.

### Ulteriori misure di sicurezza

“nessuna”, se non previste

### Adeguatezza delle misure di sicurezza

Il Fornitore è tenuto a dichiarare nel Libretto di Sistema l’adeguatezza delle Misure di Sicurezza che ha adottato per la protezione della sicurezza e della privacy in funzione dei requisiti delle attività di servizio e alla relativa classificazione di livello di criticità del sottosistema informativo oggetto dello stesso, e ad evidenziare con cadenza trimestrale, con apposita comunicazione, la loro verifica periodica. le misure di sicurezza di natura tecnica (informatica) che dovranno essere garantite sono quelle previste dal paragrafo 4 dell’articolo 28 del Regolamento Europeo 2016/679, ovvero (citazione dal GDPR):

* la pseudonimizzazione e la cifratura dei dati personali;
* la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
* la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
* una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

e/o anche quelle previste dalla Circolare ANAC 18/04/2017 n. 2/2017 relative alle Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni.

1. Cagliari, Sassari, Nuoro, Gallura, Oristano, Medio Campidano, Sulcis, Ogliastra; [↑](#footnote-ref-1)
2. Applicativi Territoriali, Applicativi Ospedalieri, Applicativi Amministrativi, Applicativi Direzionali, Infrastruttura e comunicazioni [↑](#footnote-ref-2)
3. Per la compilazione dei campi ‘Sottosistema’, ‘Codice’ fare riferimento alla tabella di specifica dei requisiti contrattuali. [↑](#footnote-ref-3)
4. Contesto: ‘Aziendale’ o ‘Aziendale–Regionale’ [↑](#footnote-ref-4)
5. Le strutture aziendali destinatarie dei servizi applicativi erogati [↑](#footnote-ref-5)
6. Il soggetto che ha in carico manutenzione e assistenza del sistema (ad esempio il fornitore) [↑](#footnote-ref-6)
7. Data aggiornamento del presente documento [↑](#footnote-ref-7)
8. ad esempio: ”su richiesta scritta del Responsabile del Trattamento del Reparto/Servizio” [↑](#footnote-ref-8)