

Congregazione delle Suore di Carità delle Sante B. Capitanio e V. Gerosa

Documento Programmatico sulla Sicurezza – Anno 2011

*ai sensi dell'art. 19 Allegato B - D.lgs. n. 196 30 giugno 2003
(Testo Unico sulla Privacy)*

Versione 3.0

**Titolare
Maria Rosa VITTONI**



Approvazione

	Ruolo	Nominativo	Data
Redatto e verificato da:	Legale Rappresentante	sr Maria Rosa VITTONI	19 marzo 2011
Approvato da:	Legale Rappresentante	sr Maria Rosa VITTONI	19 marzo 2011

Storia del documento

Nella seguente tabella si riporta la storia degli aggiornamenti, modifiche apportate nelle diverse versioni del Documento Programmatico sulla Sicurezza.

Codice Doc	Versione	Data	Commenti sulla versione
DPS – 2005	1.0	14 dicembre 2005	Prima predisposizione del DPS
DPS – 2010	2.0	19 marzo 2010	Seconda versione del documento
DPS – 2011	3.0	19 marzo 2011	Revisione a seguito cambio Legale Rappresentante



Gruppo di lavoro

Questo documento è stato redatto, nella sua versione 2.0, tramite informazioni e documentazione fornite dai responsabili delle seguenti aree aziendali o presidi della Congregazione (riportati in ordine alfabetico).

Nominativo	Ufficio	Attività svolta
Suor Rosangela ROTA	Economato Generale e rappresentanza legale	Legale rappresentante
Giancarla Suor Giuseppina CASATI	Economato ed EDP	Responsabile economato
Manuela MELE	Ufficio contabilità	Responsabile ufficio contabilità
Carlo CITTERIO	Ufficio personale	Responsabile ufficio personale
Suor Emanuela BRAMBILLA	Ufficio personale	Collaboratrice ufficio personale
Suor Augusta ZANDEGIACOMO CELLA	Economato Presidio Vicenza	Economa
Roberta GAZZOLA	Amministrazione Presidio Vicenza	Assistente part – time per l'amministrazione e contabilità del Presidio di Vicenza



CONTENUTI

1	Contesto di riferimento e ambito di applicazione	5
2	Terminologia e Definizioni	6
3	Rilevazione dello scenario	8
3.1	Struttura organizzativa	8
3.2	Infrastruttura Tecnologica.....	9
4	Censimento dei trattamenti di dati personali (regola 19.1)	12
5	Distribuzione di compiti e responsabilità (regola 19.2)	13
5.1	Modello Organizzativo interno per la tutela dei dati personali.....	13
6	Analisi dei Rischi (regola 19.3)	14
6.1	Definizioni e concetti generali	14
6.2	Classificazione dei dati personali.....	15
6.3	Domini di Rischio	16
6.4	Analisi delle Minacce e delle Vulnerabilità.....	18
6.4.1	<i>Analisi delle Minacce</i>	18
6.4.2	<i>Analisi delle Vulnerabilità</i>	19
6.4.3	<i>Valutazione dei rischi intrinseci: Fattore di Esposizione</i>	19
6.5	Analisi e Valutazione dei rischi	21
7	Misure di sicurezza predisposte o da adottare (regola 19.4)	24
8	Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)	32
9	Previsione di interventi formativi (regola 19.6)	33
10	Trattamenti di dati affidati all'esterno (regola 19.7)	34
11	Cifratura dei dati o separazione dei dati identificativi (regola 19.8)	35
12	Programma di revisione delle misure di sicurezza	366
13	Modulistica	40
	Appendice...	41

INDICE DELLE TABELLE

Tabella 1. Definizioni	7
Tabella 2. Domini di rischio	17
Tabella 3. Lista delle minacce di riferimento	18
Tabella 4. Matrice di valutazione del Fattore d'Esposizione al rischio (EF).....	20
Tabella 5. Livelli complessivi di Rischio (LdR per i domini di rischio)	22
Tabella 6. Misure minime di Sicurezza	31
Tabella 7. Programma di revisione e monitoraggio periodico delle Misure Minime di Sicurezza	39



1 Contesto di riferimento e ambito di applicazione

La normativa italiana in materia di Tutela dei dati personali definisce gli adempimenti che devono essere intrapresi per garantire la riservatezza, l'integrità e la disponibilità delle informazioni contenenti dati personali e sensibili.

Il Codice in materia di protezione dei dati personali (il D.lgs. 196/03, in seguito anche "Testo Unico" o "Il Codice") è entrato in vigore a partire dal 10 Gennaio 2004; incorpora la normativa vigente fino al 31 dicembre 2003 in materia di tutela della Privacy (in particolare la Legge 675/96 e il D.P.R. 318/99), prevedendo una serie di modifiche e aggiornamenti, sia a livello di adempimenti normativi a tutela della privacy sia per quanto riguarda l'adozione delle misure minime di sicurezza.

In particolare, in materia di protezione di dati personali, il Testo Unico, nel Titolo V (Sicurezza dei dati e dei sistemi), prevede specifici obblighi di sicurezza: l'obbligo di adozione di misure idonee atte a prevenire e ridurre al minimo i rischi di perdita di riservatezza, integrità e disponibilità dei dati personali (rif. art. 31 del Codice) e l'obbligo dell'adozione di una serie di misure minime di sicurezza (rif. artt. 33-36 del Codice).

Nell'ambito delle misure minime di sicurezza, il Testo Unico prevede, nel caso in cui si trattino in seno all'azienda dati personali sensibili su elaboratori elettronici (es: dati relativi all'appartenenza al sindacato da parte dei dipendenti, dati idonei a rivelare portatori di handicap), la predisposizione del Documento Programmatico sulla Sicurezza.

Inoltre, le seguenti specifiche disposizioni di legge o provvedimenti dell'Autorità Garante per la Privacy hanno una rilevanza diretta o indiretta in tema di predisposizione del DPS:

- il Provvedimento del Garante Privacy del 27/11/08 "*Semplificazioni in materia di Misure Minime di Sicurezza*", che prevede delle semplificazioni nell'adozione delle misure minime di sicurezza previste dal Disciplinare Tecnico (rif. Allegato B al Codice Privacy); tale Provvedimento prevede fra le altre semplificazioni, la predisposizione di un DPS semplificato nel caso in cui il titolare dovesse trattare come unici dati sensibili le categorie di dati sopra menzionate e tutti i dati di natura personale per sole finalità amministrative e contabili;
- il Provvedimento del Garante Privacy del 27/11/2008 "*Misure e accorgimenti inerenti la funzione di Amministratore di Sistema*", e sue successive modifiche, che prevede una serie di misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici, relativamente alle attribuzioni delle funzioni di amministratore di sistema.

L'ambito di applicazione di tale Documento è costituito dall'insieme dei trattamenti di dati personali effettuato dalla Congregazione presso la propria sede centrale di Milano e i propri presidi.



2 Terminologia e Definizioni

Ai fini del presente documento, si applicano alcune delle definizioni riportate nel D. Lgs. 30 giugno 2003 n.196 (in seguito Testo Unico sulla Privacy):

Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Dati giudiziari	Si tratta di dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di impuntato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Dati identificativi	Si tratta di dati personali che permettono l'identificazione diretta dell'interessato.
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 (art. 4 T.U.).
Dato sensibile	Il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale, nonché il dato personale idoneo a rivelare lo stato di salute e la vita sessuale.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Garante per la protezione dei dati personali	L'autorità, istituita ai sensi dell'articolo 153 del T.U., è un organo collegiale costituito da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. Essi eleggono al loro interno un Presidente il cui voto prevale in caso di parità. I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza nelle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.
Incaricato	La persona autorizzata dal Titolare o dal Responsabile di trattamento a compiere le operazioni di <i>trattamento</i> .
Informativa all'interessato	L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati in merito al trattamento dei dati personali, secondo quanto disposto dall'art. 13 T.U.



<i>Interessato</i>	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
<i>Misure minime</i>	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste dal Disciplinare Tecnico (Allegato B del T.U.), che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art.31, comma 1, del T.U.
<i>Notificazione del trattamento</i>	Il Titolare notifica al Garante il trattamento di dati personali cui intende procedere, secondo le disposizioni previste dall'art. 37 del T.U.
<i>Responsabile del trattamento</i>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali.
<i>Strumenti</i>	I mezzi elettronici o comunque automatizzati con cui si effettua il trattamento.
<i>Titolare</i>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare le decisioni in ordine alle finalità, alle modalità del <i>trattamento</i> di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
<i>Trattamento</i>	Qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati (art. 4 T.U.).

Tabella 1. *Definizioni*



3 Rilevazione dello scenario

3.1 Struttura organizzativa

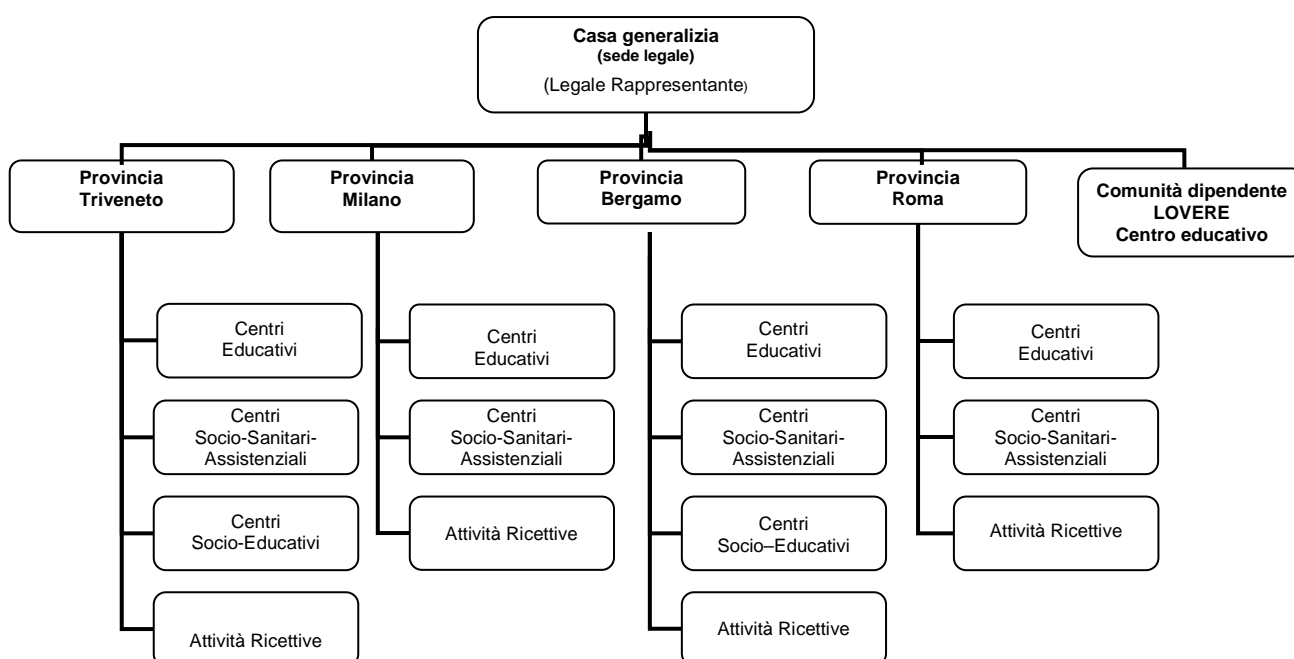
La Congregazione delle Suore di Carità delle sante B. Capitanio e V. Gerosa è un ente ecclesiastico civilmente riconosciuto ai sensi del R. D. 12 dicembre 1932 n. 2012.

La Congregazione, ai soli fini canonici, è suddivisa in Province religiose e Delegazioni. In Italia la Congregazione è attualmente divisa in 5 Province religiose e di queste fanno parte sia le attività “istituzionali”, sia le attività diverse soggette alle leggi dello Stato concernenti tali attività e al regime tributario previsto per le medesime.

Le attività così dette diverse, riconducibili alle finalità istituzionali della Congregazione, sono state raggruppate nelle seguenti macro-categorie:

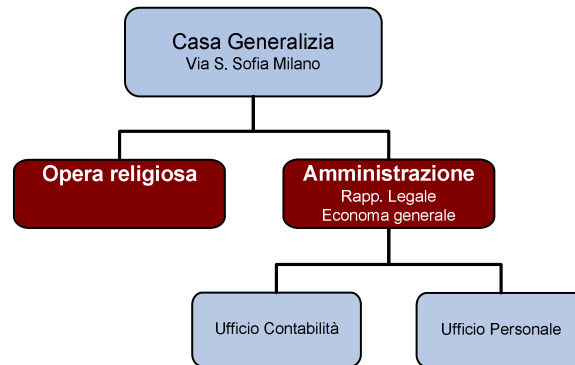
- **Centri Educativi:** offrono prestazioni educative e scolastiche attraverso strutture che ricoprono l'intero percorso di studi dell'utente, dal nido-scuola dell'infanzia alla scuola secondaria di secondo grado.
- **Centri Socio-Sanitario-Assistenziali:** offrono prestazioni sanitarie-assistenziali e sanitarie nei confronti di persone anziane autosufficienti e/o non autosufficienti e malati attraverso Residenze Socio-Sanitario e Assistenziali RSA (le quali, al loro interno, possono offrire anche servizio di Hospice per i malati terminali, Casa di riposo, ecc.)
- **Centri Socio-Educativi:** offrono servizi assistenziali al fine di favorire il recupero del benessere delle persone accolte, realizzando attività di cura e di sostegno (ad es. Centri di Pronto Intervento e Centri di Aggregazione Giovanile).
- **Attività Ricettive:** convitti per studenti e lavoratrici, centri di spiritualità, case per ferie.

La sede centrale della Congregazione è sita a Milano, in via Santa Sofia 13, mentre di seguito è riportata una rappresentazione dei presidi nelle province religiose:





Presso la sede centrale operano 4 collaboratori laici, coordinati dalla rappresentante legale della Congregazione e dall'economista generale. La composizione della Casa Generalizia è rappresentata di seguito.

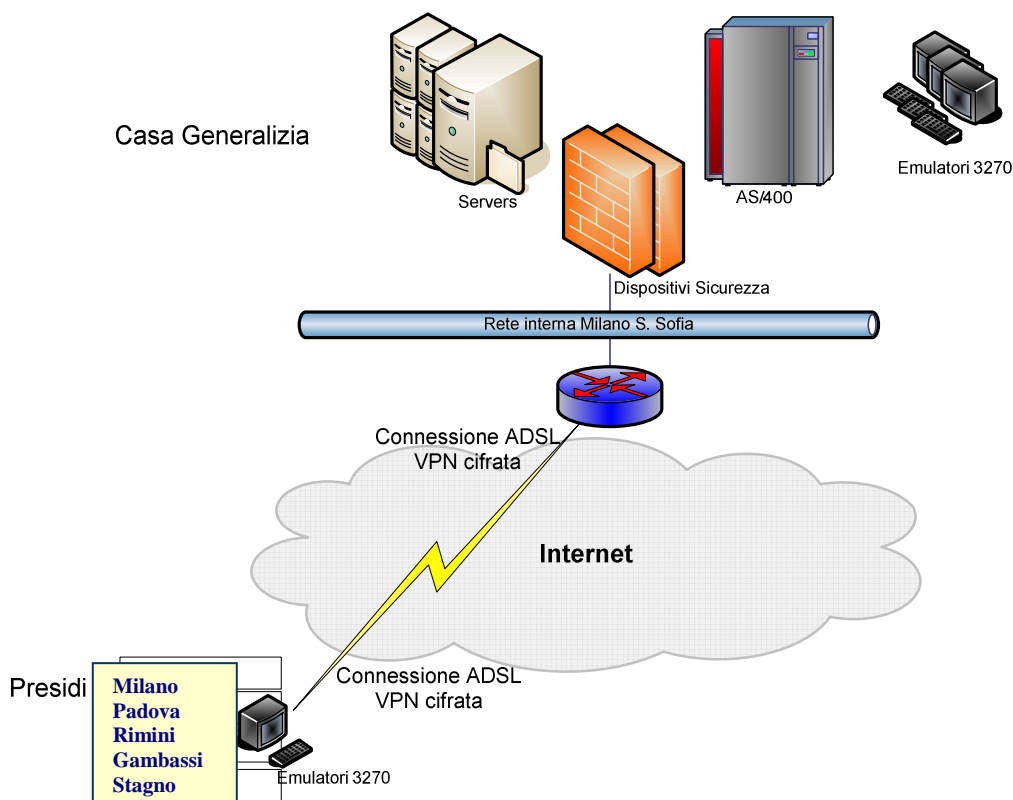


3.2 Infrastruttura Tecnologica

La sede centrale della Congregazione è sita a Milano. Presso tale sede è presente il sistema informativo centrale (il gestionale) e il file server e qui sono gestiti centralmente i trattamenti di dati dei diversi presidi, per finalità amministrative e contabili (es. fatturazione, contabilità generale, adempimenti fiscali, predisposizione del bilancio civilistico e bilancio consolidato, ecc.) e finalità di gestione del personale (payroll).

Infrastruttura di Rete

Circa la metà dei presidi dispone di un collegamento telematico a banda larga sicuro (VPN) diretto al sistema informatico gestionale presente presso la sede centrale di Milano; gli operatori dei rispettivi presidi, grazie a tale collegamento, sono in grado di inserire a sistema i dati aziendali necessari per finalità amministrative e contabili (es. registrazione fatture, prima nota, gestione personale, ecc.). Riportiamo sotto una rappresentazione dell'infrastruttura di rete della Congregazione.



I restanti presidi, che non dispongono del suddetto collegamento telematico al sistema, comunicano i dati alla sede centrale in formato cartaceo (es. prima nota, giustificativi per finalità contabili quali fatture, ricevute fiscali, ecc.).

Gli operatori di tutti i presidi dispongono di personal computer per la gestione dei dati anagrafici di alunni, dipendenti, ospiti o fornitori, tramite le comuni applicazioni di office o altre specifiche applicazioni installate direttamente sulle workstation.

Inoltre, per mezzo di tali pc e della connettività internet, riescono a ricevere le comunicazioni inviate dal MIUR (Ministero Istruzione Università Ricerca), dagli Uffici scolastici Provinciali, dalle Direzioni generali, dagli Enti locali, dalle ASL, ecc...

Sistemi IT

Il componente principale del sistema informativo della Congregazione è costituito da una piattaforma IBM I5 (AS/400) e supportato da un contratto triennale di assistenza con il produttore, su cui sono ospitati il software gestionale AGAS 2000 di Thera S.p.A., e l'applicativo per la gestione del payroll STP-25 Stipendi e Paghe di SCT Italia srl.

Sulle postazioni degli utenti abilitati all'uso di tali applicativi è presente un emulatore IBM in grado di interfacciarsi al sistema centrale di Milano; l'ambiente di lavoro delle postazioni di lavoro è costituito dal sistema Windows XP.

Il censimento delle postazioni di lavoro presenti presso la sede e diversi presidi della Congregazione è riportato nel modulo **Mpr-01: Censimento postazioni di lavoro.**



Principali applicazioni

Le applicazioni di riferimento, per quanto concerne il trattamento di dati personali, risiedono prevalentemente sulla piattaforma AS/400 e riguardano:

- gestione stipendi e paghe
- contabilità clienti
- contabilità fornitori

Nel modulo **Mpr-02 Censimento dei trattamenti elettronici e cartacei**, sono descritte sul piano funzionale tali applicazioni, insieme ad altre applicazioni installate sui pc degli operatori, riportando anche le aree aziendali che principalmente le utilizzano.

La Congregazione, per determinati trattamenti di dati, si avvale anche di altre applicazioni, il cui client è installato sui pc degli operatori, fornite da terze società.



4 Censimento dei trattamenti di dati personali (regola 19.1)

La Congregazione, nell'ambito delle proprie attività lavorative, effettua trattamenti di dati personali con o senza l'ausilio di strumenti elettronici.

Al fine di comprendere gli ambiti, le modalità e le finalità di trattamento, sono stati censiti ad alto livello gli archivi sia elettronici che cartacei contenenti dati personali.

Per ciascuna tipologia di archivio cartaceo e/o di base dati elettronici, sono stati individuati:

- la denominazione dell'archivio;
- i soggetti interessati dal trattamento dei dati;
- la categoria di dati personali contenuti in ciascuno di tali archivi (dati Sensibili e/o Giudiziari o altri dati personali non sensibili, definibili come dati "Comuni");
- le finalità e le modalità di trattamento;
- le applicazioni coinvolte nel trattamento;
- il riferimento alle piattaforme che ospitano le applicazioni coinvolte;
- la localizzazione fisica degli archivi, ossia gli uffici dove fisicamente sono custoditi gli archivi (in caso di trattamento cartaceo);
- le modalità adottate di custodia e conservazione dei dati (in caso di trattamento cartaceo);
- le applicazioni che utilizzano ed elaborano i dati contenuti nella base dati;
- le piattaforme tecnologiche (sistemi e database) su cui girano le applicazioni e vengono memorizzati i dati.

I risultati del censimento dei trattamenti elettronici e cartacei sono riportati nel modulo **Mpr-02: Censimento dei trattamenti elettronici e cartacei**.



5 Distribuzione di compiti e responsabilità (regola 19.2)

5.1 Modello Organizzativo interno per la tutela dei dati personali

Per far fronte agli adempimenti che discendono dal Testo Unico, la Congregazione ha definito uno specifico modello organizzativo provvedendo ad individuare le figure previste dalla Legge:

- Titolare dei trattamenti;
- Responsabile dei trattamenti (interno ed esterno);
- Incaricati del trattamento (interni ed esterni).

La responsabilità primaria della tutela dei dati personali gestiti dalla Congregazione fa capo al Titolare.

Titolare del trattamento dei dati, ai sensi dell'Art. 28 del Testo Unico, è la **Congregazione delle Suore di Carità delle Sante B. Capitanio e V. Gerosa**, con sede centrale in Milano, nella figura della rappresentante legale.

Al Titolare competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza e l'assegnazione e la revoca delle autorizzazioni ai Responsabili dei trattamenti delle banche dati personali.

Il Titolare ha nominato i **Responsabili interni del Trattamento Dati (RTD)** dei singoli presidi. Gli RTD sono stati designati ai sensi dell'art.29 del Testo Unico (definendone i compiti e le istruzioni cui gli stessi devono attenersi per trattare i dati delle aree di propria competenza). **Mpr-03/01: Nomina responsabili interni del trattamento dati.**

Il Responsabile del trattamento deve assicurare, per l'area di competenza attribuita, il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali presente e futuro, per tutto il ciclo di loro utilizzazione, come stabilito dal Testo Unico, curando la programmazione e l'attuazione degli interventi utili a garantire la sicurezza dei dati stessi.

Gli **Incaricati** sono coloro che, per l'espletamento della loro attività aziendale, sono autorizzati dal relativo Responsabile ad accedere ed utilizzare le risorse informative, secondo quanto da lui stabilito. **Mpr-04/01: Nomina incaricati interni al trattamento dati.**

Ogni Incaricato, cui è concesso il diritto di accesso ai dati, si assume anche la responsabilità.

In particolare, è tenuto a:

- adottare tutte le possibili cure ed attenzioni nello svolgimento delle operazioni di trattamento dei dati personali;
- trattare i dati solo ed esclusivamente per gli scopi inerenti alla propria attività, attenendosi alle istruzioni impartite e nei limiti delle autorizzazioni concesse dal Responsabile;
- non diffondere o comunicare a terzi i dati di cui viene a conoscenza, al di fuori dei casi consentiti dal Testo Unico e in conformità alle norme e procedure aziendali;
- segnalare prontamente al proprio Responsabile ogni tentativo di violazione, illecito, errore e anomalia riscontrati;
- adottare le idonee misure di sicurezza per il trattamento dei dati memorizzati e gestiti localmente su PC.



6 Analisi dei Rischi (regola 19.3)

L'analisi dei rischi è stata effettuata in conformità a quanto richiesto dal Codice in materia di protezione dei dati personali, allegato B “*Disciplinare Tecnico in materia di misure minime di sicurezza*” al punto 19.3.

Nello specifico, partendo dalla valutazione della criticità delle informazioni presenti nell'Ente sotto il profilo della Privacy, sono state considerate le possibili minacce a cui esse possono essere esposte ed il livello di vulnerabilità considerato rispetto alle contromisure in essere. Tale analisi è stata condotta al fine di definire le appropriate misure di sicurezza da adottare per far fronte ai vari tipi di rischio cui sono soggetti i dati e i sistemi.

Il perimetro di intervento oggetto dell'analisi dei rischi è rappresentato dalla Congregazione. I risultati dell'analisi forniscono informazioni di supporto per valutare lo stato di implementazione dei controlli e di conseguenza le aree in cui sono maggiormente individuabili le opportunità di miglioramento mediante l'implementazione di misure idonee come richiesto dal D. Lgs. 196/03.

In particolare, l'analisi dei rischi viene effettuata allorché vengono sviluppati, acquisiti o installati nuovi sistemi hardware, software o applicazioni, e ogni qualvolta avvengano cambiamenti significativi dei sistemi.

L'analisi dei rischi effettuata dalla Congregazione è articolata nella seguente struttura:

1. definizioni e concetti generali;
2. classificazione delle informazioni (dati personali);
3. individuazione delle minacce/vulnerabilità;
4. valutazione del rischio.

6.1 Definizioni e concetti generali

Sulla base di quanto indicato da numerosi standard internazionali in tema di gestione della sicurezza delle informazioni (ITSEC, Common Criteria, ISO 27000, etc.), si individuano i seguenti tre parametri/requisiti di sicurezza per le informazioni:

Riservatezza:

Tale requisito, specificatamente indicato nelle finalità previste dal Testo Unico, si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati da modalità di trattamento non autorizzato (rischio di accesso ai dati da parte di soggetti non autorizzati). Tale requisito di sicurezza è ravvisabile nelle attività qui di seguito riportate (indicate espressamente dal Testo Unico):

- ✓ Raccolta;
- ✓ Registrazione,
- ✓ Organizzazione;
- ✓ Conservazione;
- ✓ Comunicazione;
- ✓ Diffusione;
- ✓ Selezione;



- ✓ Estrazione;
- ✓ Raffronto;
- ✓ Interconnessione;
- ✓ Utilizzo.

Integrità:

Tale requisito si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati da modalità di trattamento non autorizzate, in particolare, contro il rischio di modifica non autorizzata delle informazioni stesse. Tale requisito di sicurezza è ravvisabile nelle attività qui di seguito riportate (indicate espressamente dal Testo Unico):

- ✓ Elaborazione;
- ✓ Modifica;
- ✓ Cancellazione;
- ✓ Distruzione.

Disponibilità:

Tale requisito, si riferisce alla necessità di intraprendere azioni in grado di proteggere i dati da possibili eventi in grado di ridurre la capacità dell'Ente di assolvere, per tempo, alle finalità di trattamento per cui tali dati sono stati raccolti oppure per evitare che l'Ente non sia in grado di fornire i dati agli interessati al trattamento che ne facciano esplicita richiesta.

In ambito Privacy, oltre che considerare nello svolgimento dei trattamenti la salvaguardia dei requisiti di sicurezza esposti, è necessario garantire il principio di “necessità del trattamento”. Nello specifico il D.Lgs 196/03 definisce che “...i sistemi informativi e i programmi informatici debbano essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.”

E' inoltre richiesta dalla normativa la garanzia che “il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali”.

6.2 Classificazione dei dati personali

Al fine di predisporre un piano di protezione in linea con le effettive esigenze, in primo luogo occorre valutare il valore delle informazioni, ossia determinare il livello di criticità del dato in termini di riservatezza, integrità e disponibilità.

Una volta eseguite tali considerazioni, si dispone di un metodo per Classificare le Informazioni Aziendali in più categorie, per le quali è poi possibile stabilire opportune misure omogenee di controllo e protezione.

In termini di privacy, la Classificazione delle Informazioni porta a stabilire quali delle Informazioni Aziendali ricadono in una delle possibili categorie:

- ✓ dati personali Sensibili e/o Giudiziari;
- ✓ dati personali non-sensibili;
- ✓ altro.



La presente analisi essendo svolta nel rispetto della normativa Privacy ha come oggetto unicamente la gestione delle informazioni relative ai trattamenti di dati personali Sensibili e/o Giudiziari e dati personali non-sensibili.

La classificazione delle Informazioni in tema di protezione della privacy e la mappatura delle categorie di dati personali con i relativi sistemi di trattamento elettronico e/o cartaceo sono illustrate nei relativi moduli (Mpr-02).

6.3 Domini di Rischio

Il modello dell'analisi dei rischi prevede di valutare le minacce e le vulnerabilità associate a domini di rischio, ossia contesti operativi in cui le informazioni aziendali vengono trattate (in particolare informazioni di natura personale ai sensi della normativa sulla privacy).

La definizione di opportuni *Domini di Rischio* ha lo scopo di:

- ✓ analizzare problematiche di sicurezza omogenee all'interno di contesti (i.e. Domini) omogenei;
- ✓ individuare controlli di sicurezza condivisibili all'interno dei Domini, favorendo quindi il processo di gestione dei rischi.

I Domini di Rischio si definiscono a partire dalle seguenti considerazioni:

- ✓ i componenti del generico Dominio di Rischio sono soggetti alle medesime tipologie di minacce e vulnerabilità;
- ✓ la suddivisione in Domini di Rischio del sistema informativo rispecchia la visione aziendale di gestione delle informazioni;
- ✓ ogni Risorsa Informativa (sia di tipo cartaceo sia di tipo informatico) si mappa in uno ed un solo Dominio di Rischio;
- ✓ l'unione dei Domini di Rischio comprende tutte le componenti dei Sistemi Informativi della Congregazione.

Al fine di svolgere in maniera consistente l'analisi delle minacce e delle vulnerabilità per il sistema di gestione delle informazioni per la Congregazione, sono stati individuati i seguenti *Domini di Rischio*.



Denominazione del contesto (Dominio di rischio)	Tipologia di trattamento dati	Descrizione delle componenti del contesto
PC in rete presso i Presidi	Elettronico	I PC in rete locale presso i presidi su cui installato: - S.O. Windows XP - i client di connessione all'AS400 Su alcuni pc possono essere presenti dati sensibili di pazienti / ospiti / alunni.
AS400	Elettronico	1 AS400 Applicazioni: - STP-25 (paghe e presenze) - AGAS 2000 I dati sensibili riguardano in particolare i dati relativi alle trattenute sindacali dei dipendenti e i dati sullo stato di salute.
Archivi Cartacei	Cartaceo	Archivi cartacei di dati personali presenti nella sede centrale di Milano (archivio ufficio Paghe e archivio Ufficio Amministrazione) e presso le sedi dei diversi presidi della Congregazione (Segreterie didattiche e amministrative delle Scuole, Economato e Reparti di Assistenza delle Case ricettive e Case di Riposo) I dati sensibili dei pazienti /ospiti /alunni presso i vari presidi. I dati sensibili cartacei dei dipendenti sono presenti nelle copie delle buste paghe archiviate presso la sede centrale di Milano.

Tabella 2. *Domini di Rischio*

Per ognuno di tali domini di rischio sono stati analizzati i fattori di esposizione alle minacce e vulnerabilità, valutando per ogni Dominio i controlli di sicurezza implementati, come di seguito illustrato.



6.4 Analisi delle Minacce e delle Vulnerabilità

6.4.1 Analisi delle Minacce

Il processo di analisi delle minacce alle Informazioni Aziendali (dati di natura personale) riguarda l'identificazione, selezione e valutazione delle possibili problematiche cui le informazioni risultano esposte, sulla base dei Domini di Rischio di appartenenza, ovvero dell'ambiente in cui operano e dei dati statistico/storici disponibili.

Una minaccia è qualsiasi insidia, pericolo o evento che possa causare:

- la distruzione, anche accidentale, dei sistemi e dei dati;
- la perdita o l'indisponibilità dei dati;
- l'accesso non autorizzato ai dati;
- il trattamento non consentito o illecito dei dati;
- la perdita di integrità dei sistemi e dei dati;
- qualsiasi altra situazione che provochi un danno alla Società.

Considerando lo scenario di riferimento della Congregazione, sono state identificate e selezionate le minacce considerate significative rispetto agli effetti che il loro concretizzarsi potrebbe avere in termini di perdita di riservatezza, disponibilità ed integrità dei dati personali gestiti dall'Ente.

Le minacce analizzate appartengono alle categorie riportate nella tabella a seguire.

Minaccia	Descrizione
Mancata reazione a incidenti o guasti	Incidenti e guasti potrebbero ripetutamente compromettere la sicurezza delle informazioni senza che le loro cause vengano rimosse.
Modifiche non autorizzate	Utenti, amministratori o sviluppatori potrebbero effettuare modifiche non autorizzate a software applicativo o di sistema o più in generale a risorse di elaborazione.
Accesso logico non autorizzato	Entità avverse potrebbero accedere senza autorizzazione ad informazioni compromettendone la sicurezza.
Codice malevolo	Entità avverse potrebbero introdurre codice malevolo (virus, worm, Trojan Horse, ecc.) nei sistemi aziendali compromettendo la sicurezza delle informazioni e dei sistemi
Compromissione dei dati durante lo scambio	Entità avverse (inclusi i partecipanti allo scambio di informazioni) potrebbero compromettere la sicurezza di dati o software scambiati tra organizzazioni o individui.
Errori umani	Amministratori, manager, incaricati, ecc., potrebbero commettere errori, con conseguente compromissione di informazioni e/o sistemi.
Accesso fisico non autorizzato	Entità avverse potrebbero rubare informazioni e apparecchiature ICT, provocare guasti o malfunzionamenti o compiere atti di sabotaggio di altra natura accedendo fisicamente ai locali che ospitano risorse elaborative, archivi, etc.
Eventi disastrosi (incendi, allagamenti, etc.)	Eventi disastrosi di grande portata potrebbero danneggiare il patrimonio informativo aziendale nonostante le misure di protezione attuate.

Tabella 3. Lista delle minacce di riferimento.



Queste minacce costituiscono le problematiche di sicurezza considerato in fase di analisi dei rischi, per valutare l'adeguatezza delle attuali misure di protezione messe in atto per le informazioni e dati personali.

La valutazione delle minacce avviene in questo contesto considerando la probabilità di accadimento delle stesse e viene espressa sulla base della seguente scala qualitativa:

- Alta
- Media
- Bassa
- Ininfluyente.

6.4.2 Analisi delle Vulnerabilità

Il processo di analisi delle vulnerabilità è inteso, a questo livello di analisi, come il processo di analisi e valutazione dello stato dell'implementazione dei controlli di sicurezza, all'interno dei vari Domini di Rischio del Sistema di Gestione della Sicurezza delle Informazioni Aziendali.

Allo scopo di avere una base di partenza stabile e successivamente confrontabile, per ciascun Dominio di Rischio definito all'interno dei Sistemi Informativi Aziendali, lo stato di definizione e attuazione dei controlli viene valutato seguendo lo schema proposto da:

- ✓ Misure Minime di Sicurezza (ai sensi dell'allegato B al D.Lgs.196/03);
- ✓ Standard BS 7799-1/ISO 17799 (ora standard ISO 27001-2).

Le vulnerabilità sono state valutate, utilizzando come riferimento gli standard e normative citate, sulla base della seguente scala qualitativa:

- *Alta*
 - assenza di misure, nessuna politica o procedura specificate
- *Media*
 - presenza di alcune misure, nessuna politica o procedura specificate
- *Bassa*
 - presenza di misure specifiche, politiche e/o procedure formalizzate
- *Ininfluyente*
 - presenza di misure specifiche, politiche e/o procedure formalizzate e periodicamente verificate.

6.4.3 Valutazione dei rischi intrinseci: Fattore di Esposizione

Il fattore di esposizione al rischio (EF) è il parametro che valuta, a fronte di una minaccia, la possibilità che questa possa effettivamente attuarsi, ovvero produrre effetti indesiderati sui sistemi e sulle informazioni (p.e. perdita di informazioni, divulgazione di informazioni a competitor, etc.).

Nel modello di analisi e valutazione dei rischi si prevede di correlare l'insieme delle vulnerabilità con l'insieme delle minacce, per valutare puntualmente, per ogni minaccia, quello che viene indicato come *fattore di esposizione al rischio (EF)*.



Generalmente, si possono intravedere uno o più controlli applicabili allo scopo di diminuire il rischio relativo alla specifica minaccia.

Quindi, nel computo dell'EF il livello di vulnerabilità è dato dalla media di quelle associate alla specifica minaccia e allo specifico Dominio di Rischio. Tale **livello medio di vulnerabilità** viene indicato con la sigla **LV**.

La valutazione del parametro EF, relativo a ciascuna minaccia, avviene tramite la correlazione del valore valutato per la minaccia (P_{min}) e il valore medio ottenuto per le vulnerabilità ad essa correlate (LV).

I valori assunti dall'EF vengono calcolati tramite la seguente matrice di valutazione del fattore di esposizione al rischio.

Livello Vulnerabilità (LV) Probabilità Minaccia (P_{Min})	Ininfluente (I)	Basso (B)	Medio (M)	Alto (A)
Ininfluente (I)	I	I	I	I
Bassa (B)	I	B	B	M
Media (M)	I	M	M	A
Alta (A)	B	M	A	A

Tabella 4. *Matrice di valutazione del Fattore d'Esposizione al rischio (EF)*

L'analisi dell'ambiente operativo della Congregazione ha permesso di valutare i livelli di EF medi per ciascuna minaccia per ciascun Dominio di Rischio analizzato. Tali livelli sono riportati nella tabella 4.



6.5 Analisi e Valutazione dei rischi

Le valutazioni delle criticità associate alle Informazioni e delle minacce e delle vulnerabilità associate ai Domini di Rischio, cui le Informazioni di natura personale e quindi le Informazioni appartengono, vengono valutate in questo contesto in maniera unificata, per fornire il risultato complessivo dell'analisi dei rischi.

Sulla base dello schema di classificazione dei dati secondo la normativa in tema di protezione della privacy, illustrato in precedenza, i livelli di rischio relativi ai dati personali e alle infrastrutture IT e all'ambiente operativo della Congregazione dipendono dalla natura dei dati personali, oltre che dai rischi intrinseci dovuti allo scenario in cui attualmente vengono gestiti, elaborati, trasmessi e memorizzati tali dati.

Nel caso di contesti di rischio con dati sensibili, il **livello di rischio (LdR)** è stato incrementato al valore superiore a quello del **Livello di Esposizione (EF)**, quest'ultimo calcolato in base alla relazione esistente fra LM e LV (es: se EF è pari a B, in caso di dominio con dati sensibili o giudiziari, il LdR è pari a M, altrimenti assume lo stesso valore di EF, ossia in presenza di soli dati personali comuni non sensibili).

La successiva tabella illustra le valutazioni ottenute dalla Congregazione nell'Analisi dei Rischi per le proprie infrastrutture e processi di gestione delle informazioni Aziendali.

Ogni casella contiene l'indicazione del livello di rischio valutato per le piattaforme e gli archivi della Congregazione, relativamente a ciascuna delle tipologie di minacce applicabili (qualora la minaccia non sia applicabile, la corrispondente casella contiene la dicitura "N/A").

I livelli di rischio sono anch'essi valutati qualitativamente, secondo la seguente scala:

- ✓ Rischio Alto (A);
- ✓ Rischio Medio (M);
- ✓ Rischio Basso (B);
- ✓ Rischio Ininfluyente (I);
- ✓ Non Applicabile (N/A).

Nella tabella a seguire i livelli di Rischio (LdR relativo a ciascun dominio di rischio) sono stati evidenziati con diverso colore, come segue:

- ✓ Bianco se Ininfluyente o Non applicabile (N/A);
- ✓ Verde se Basso;
- ✓ Giallo se Medio;
- ✓ Rosso se Alto.

I domini di rischio che comprendono trattamenti di dati personali sensibili sono stati evidenziati in giallo nella testata della tabella.



Minacce/problematiche sicurezza	PC presso i presidi				AS400 – LAN Milano				CONTESTO CARTACEO			
	LdR	EF	LM	LV	LdR	EF	LM	LV	LdR	EF	LM	LV
<i>Mancata reazione a Incidenti o Guasti</i>	M	B	B	M	B	B	B	B	N/A	N/A	N/A	N/A
<i>Modifiche non autorizzate</i>	A	A	M	A	A	M	B	A	B	I	I	B
<i>Accesso logico non autorizzato</i>	A	A	M	A	A	M	M	A	N/A	N/A	N/A	N/A
<i>Codice Malevolo</i>	B	B	B	B	M	B	B	B	N/A	N/A	N/A	N/A
<i>Compromissione dei dati durante lo scambio</i>	B	B	B	B	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<i>Errori Umani</i>	A	A	A	M	A	A	A	M	B	I	I	B
<i>Accesso fisico non autorizzato</i>	M	B	B	M	M	B	B	M	B	I	I	M
<i>Eventi disastrosi</i>	B	B	B	B	B	B	B	B	B	I	I	M

Tabella 5. Livelli complessivi di Rischio (LdR per i domini di rischio)



La tabella riporta un quadro di rischio complessivamente Medio; tale valutazione deriva dalla natura del lavoro svolto dall'Ente, e i relativi rischi sono presi in dovuta e adeguata considerazione dall'Ente (si veda lo stato di adozione delle misure in essere e la previsione di interventi correttivi descritta in capitolo 6).

A fronte di tali potenziali minacce, l'Ente ha già predisposto alcune misure e intende predisporre l'adozione di altre al fine di ridurre ulteriormente l'esposizione al rischio (si veda capitoli 7 e 8).

In particolare, l'Ente pone ulteriore enfasi sulla necessità di ridurre, con riferimento a determinati domini di rischio, e quindi contesti tecnologici di riferimento, l'esposizione al rischio determinata rispetto alle minacce derivanti da "Errori umani"; "Accessi logici non autorizzati" e "Modifiche non autorizzate".



7 Misure di sicurezza predisposte o da adottare (regola 19.4)

In tale capitolo si riportano le misure di sicurezza (soluzioni tecniche e organizzative) adottate dalla Congregazione a protezione dei dati personali suddivise per categorie di controlli (sulla base dello schema proposto dallo standard ISO 27001-2).

La terza colonna della tabella a seguire riporta l'eventuale corrispondenza di alcuni dei controlli di sicurezza implementati dalla Congregazione con le disposizioni in materia di contenuto minimo previsto nel DPS (tali disposizioni sono contenute all'interno della regola 19 dell'Allegato B del D.Lgs. 196/03).

La quarta colonna riporta l'eventuale corrispondenza di alcuni dei controlli di sicurezza implementati dalla Congregazione con le disposizioni del D. Lgs. 196/03 (in seguito T.U.) e dell'Allegato B dello stesso Decreto, in tema di obblighi di adozione di misure di sicurezza.



Categorie di controlli	Controlli/Misure Implementate	Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)	Rif. T.U. e Allegato B del T.U.	Misure da adottare
Organizzazione della Sicurezza	<ul style="list-style-type: none"> ▪ Modello organizzativo per la protezione dei dati personali [v. sezione 5.1.DPS] 	19.2. – “Distribuzione di compiti e responsabilità”.	<ul style="list-style-type: none"> ▪ Artt. 28-30 T.U. ▪ Regola19 Allegato B T.U. 	Aggiornamento sistematico del corpo documentale degli atti di nomina degli incaricati di tutti i presidi della Congregazione
Gestione dei beni e della strumentazione informatica (asset informatici)	<ul style="list-style-type: none"> ▪ Censimento e classificazione di dati personali e mappatura su sistemi IT e archivi cartacei [v. sezione 4 DPS] 	19.1 – “Elenco dei trattamenti di dati personali	<ul style="list-style-type: none"> ▪ Regola 19- Allegato B T.U. 	Aggiornamento sistematico dell’inventario degli asset informatici presenti presso i vari presidi della Congregazione (pc, server, apparati di rete)



<i>Categorie di controlli</i>	<i>Controlli/Misure Implementate</i>	<i>Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)</i>	<i>Rif. T.U. e Allegato B del T.U.</i>	<i>Misure da adottare</i>
<p>Sicurezza Ambiente di lavoro</p>	<ul style="list-style-type: none"> ▪ Distribuzione di norme comportamentali (vedi istruzione operativa incaricato – allegato B), per corretto svolgimento dell’attività lavorativa e il corretto utilizzo dei sistemi informativi <ul style="list-style-type: none"> - gestione dei supporti removibili (prevedendo la formattazione, se non la distruzione, al fine di evitare utilizzi impropri) - accesso sicuro agli archivi cartacei - gestione delle credenziali di accesso - accesso sicuro alle postazioni di lavoro e ai servizi quali posta elettronica, internet, ecc. - esecuzione di scansioni antivirus. ▪ Definizione delle responsabilità per l’assegnazione, la modifica e la revoca delle utenze e dei diritti di accesso a sistemi e applicazioni aziendali (vedi atti di nomina a responsabile del trattamento) 	<p>19.6 – “Previsione di interventi formativi degli incaricati”.</p>	<ul style="list-style-type: none"> ▪ Regole 4, 9,21,22, 27- Allegato B T.U. 	<p>Definizione e attuazione di un piano di formazione specifica in tema di sicurezza e privacy dei dati.</p>



Categorie di controlli	Controlli/Misure Implementate	Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)	Rif. T.U. e Allegato B del T.U.	Misure da adottare
Sicurezza fisica e controlli ambientali	<ul style="list-style-type: none"> ▪ Controllo degli accessi fisici alla sede, tramite identificazione dei visitatori all'ingresso. ▪ Presenza di armadi (dove custoditi archivi cartacei di dati personali) in uffici chiusi a chiave in assenza di personale in servizio. ▪ Istruzioni operative impartite agli incaricati per la protezione fisica delle postazioni di lavoro (i.e. protezione della sessione di trattamento attiva, restrizione dell'accesso ai soli dati necessari per espletare i propri compiti, blocco dell'elaboratore, ecc.). 	<p>19.4 – “Misure per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità”.</p>	<ul style="list-style-type: none"> ▪ Regole 28, 29- Allegato B T.U. 	



Categorie di controlli	Controlli/Misure Implementate	Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)	Rif. T.U. e Allegato B del T.U.	Misure da adottare
<p>Gestione delle comunicazioni e dei sistemi informatici</p>	<ul style="list-style-type: none"> ▪ Adozione soluzione antivirus su pc e server windows, con aggiornamento automatico giornaliero (con cadenza sempre inferiore al semestre e comunque ogni volta che l'automatismo rileva la disponibilità di un nuovo aggiornamento) ▪ Servizio fornito dalla Telecom di antispam e web content filtering, applicato sui sistemi di sicurezza perimetrale (firewall CISCO PIX 515 e soluzione IPS della fortinet) ▪ Soluzione firewall e IP ▪ Istruzioni operative agli incaricati per la corretta pianificazione ed esecuzione di scansioni antivirus. ▪ Aggiornamento periodico del file server tramite servizio di distribuzione delle patch di sistema. ▪ Adozione di soluzione VPN per la sicurezza negli scambi di dati via internet. ▪ Amministrazione dei sistemi via remota da parte di terzi fornitori di servizi informatici 	<p>19.4 – “Misure per garantire l'integrità e la disponibilità dei dati”</p>	<ul style="list-style-type: none"> ▪ Regole 16,17,18- Allegato B T.U. 	



Categorie di controlli	Controlli/Misure Implementate	Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)	Rif. T.U. e Allegato B del T.U.	Misure da adottare
<p>Controllo degli accessi</p>	<ul style="list-style-type: none"> ▪ Autenticazione con User ID e password per i pc in rete e per l'AS400 ▪ Istruzioni agli incaricati preposti al trattamento al fine di sensibilizzarli sulla corretta definizione e gestione delle credenziali di accesso ai sistemi (vedi regolamento utente) ▪ Uno stesso utente non ha più credenziali di accesso su stesso sistema. ▪ Garantita la disponibilità degli accessi su AS400, grazie al supporto del fornitore Thera. ▪ Definizione di profili utente sulla base di un sistema di autorizzazione e comunque prima dell'inizio dei trattamenti (sulla base della mappatura dei trattamenti, come da descrizione riportata nella sezione 5 di tale documento). ▪ L'accesso ad internet è consentito solo per esigenze lavorative e ai soli utenti autorizzati. 	<p>19.4 – “Misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità”.</p>	<ul style="list-style-type: none"> ▪ Regole 1, 2, 3, 5, 6, 7, 8, 10, 12, 13, 14, 15, 20- Allegato B T.U. 	<p>Adeguamento del sistema di autenticazione e autorizzazione dell'accesso al sistema AS400 e ai personal computer.</p>



Categorie di controlli	Controlli/Misure Implementate	Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)	Rif. T.U. e Allegato B del T.U.	Misure da adottare
Manutenzione e sviluppo dei sistemi informatici	<ul style="list-style-type: none"> Non applicabile e non richiesto rispetto alle disposizioni di legge in tema di privacy. 		Art. 31 T.U. (adozione di misure di sicurezza, al fine di ridurre i rischi informatici).	
Gestione degli incidenti di sicurezza	<ul style="list-style-type: none"> Non applicabile e non richiesto rispetto alle disposizioni di legge in tema di privacy. 		Art. 31 T.U. (adozione di misure di sicurezza, al fine di ridurre i rischi informatici).	
Gestione dell'emergenza e della continuità operativa	<ul style="list-style-type: none"> Si rimanda per dettagli alla sezione 8 di tale documento. 	19.5 – “Misure per il ripristino, entro massimo 7 giorni, della disponibilità dei dati in seguito a distruzione o danneggiamenti”	<ul style="list-style-type: none"> Regola 23– Allegato B T.U. 	Formalizzazione della procedura di backup dei dati dell'AS 400.



<i>Categorie di controlli</i>	<i>Controlli/Misure Implementate</i>	<i>Disposizione su contenuto minimo DPS (regola 19 Allegato B – D. Lgs. 196/03)</i>	<i>Rif. T.U. e Allegato B del T.U.</i>	<i>Misure da adottare</i>
Conformità a normative e leggi	<ul style="list-style-type: none"> ▪ Aggiornamento periodico dei DPS ai sensi D.Lgs. 196/03. ▪ Adeguamento agli adempimenti previsti dalla normativa sulla privacy. ▪ Impartite istruzioni agli incaricati al fine di attuare il divieto di utilizzare software non ufficialmente rilasciato dalle apposite strutture interne. ▪ Definizione e attuazione di programmi di revisione periodica delle misure di sicurezza. ▪ Dichiarazione di conformità alle MMS previste dalla normativa sulla privacy, richieste a terzi fornitori nel caso in cui implementino misure di sicurezza per conto del Titolare di trattamento. 		<ul style="list-style-type: none"> ▪ Regole 19, 25, 26 – Allegato B T.U. ▪ Artt 31-33 T.U. 	

Tabella 6. *Misure minime di Sicurezza*

8 Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

La Congregazione adotta le seguenti procedure e contromisure per assicurare la disponibilità dei dati in caso di loro distruzione e/o danneggiamento:

- il backup dei dati effettuato su nastri dell'AS400 presente nella sede di Milano
- il backup dei dati su cd-rom del file server presente nella sede di Milano. In tale server sono archiviati i file degli operatori delle diverse aree aziendali.

Ogni incaricato, qualora sia possibile in base alle dotazioni sw e hw a disposizione, è tenuto a predisporre il salvataggio di copie di eventuali file archiviati in locale sulla propria macchina.

Non è stato al momento formalizzato un piano e relative procedure operative per il Disaster Recovery; la direzione della Congregazione ha valutato, in base all'analisi dei rischi, che la procedura di backup dei dati del sistema centrale AS400 sia sufficiente per garantire il ripristino della disponibilità dei dati entro i termini stabiliti dalla normativa sulla privacy (entro 1 settimana).

9 Previsione di interventi formativi (regola 19.6)

L'obiettivo del programma è la realizzazione di interventi formativi dei responsabili e degli incaricati al trattamento volti ad aumentare la consapevolezza dei rischi relativi all'utilizzo dei dati aziendali e degli strumenti disponibili per prevenire incidenti di sicurezza.

Il programma di formazione e sensibilizzazione comprende in particolare le norme comportamentali sulla protezione dei dati personali più rilevanti in rapporto alle relative mansioni aziendali, le responsabilità che derivano dall'utilizzo dei sistemi informatici e le modalità per aggiornarsi sulle misure minime adottate dal titolare.

10 Trattamenti di dati affidati all'esterno (regola 19.7)

La Congregazione, in qualità di Titolare del trattamento dei dati personali, ha individuato le strutture esterne che concorrono al trattamento dei dati, come ad esempio:

- Fornitori di servizi informatici
- Studio esterno Dott. Commercialista, per l'assistenza contabile e fiscale
- Unità Sanitarie Locali, nell'ambito della gestione delle convenzioni da parte delle Case ricettive e Case di Riposo
- MIUR (Ministero Istruzione Università e Ricerca), USR (Uffici Scolastici Regionali), Regioni, Comuni (...) nell'ambito della gestione di contributi, convenzioni e adempimenti in materia di legislazione scolastica.

Ogni presidio ha la responsabilità di gestire l'assegnazione delle responsabilità privacy a tutte quelle terze strutture che concorrono al trattamento dei propri dati di natura personale, per conto della Congregazione.

La responsabilità di tali entità ai fini della tutela dei dati personali di cui la Congregazione è Titolare, è stata definita e perfezionata all'interno di appositi contratti di servizi e/o lettere di nomina a Responsabile esterno preposto al trattamento dei dati personali, ai sensi dell'art. 29 del Testo Unico.

11 Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

La regola 19.8 dell'Allegato A del D. Lgs. 196/03 prevede l'individuazione e descrizione delle modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura o la separazione fra dati identificativi e dati sensibili, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti.

Gli archivi contenenti dati sensibili (in particolare presso le Case di Assistenza e di riposo) sono tenuti separati dagli altri tipi di archivi contenenti dati non sensibili.



12 Programma di revisione delle misure di sicurezza

Per assicurare la corretta applicazione delle misure minime di sicurezza a protezione dei dati è stato predisposto un programma per la realizzazione, con differente periodicità, di attività di verifica.

<i>Attività di Verifica</i>	<i>Ambiente informatico interessato</i>	<i>Frequenza</i>	<i>Rif. Testo Unico Privacy</i>	<i>Evidenza oggettiva dell'attività</i>
Verifica e aggiornamento del Documento Programmatico sulla Sicurezza (DPS)	Tutti i sistemi informatici che supportano il trattamento di dati personali.	Annuale	Allegato B, MMS 19	Sezione iniziale del DPS “Storia del Documento”, che tiene traccia di tutti gli aggiornamenti effettuati.
Analisi dei rischi per la sicurezza dei dati di natura personale (ambito privacy).	Tutti i sistemi informatici che supportano il trattamento di dati personali.	Annuale	Allegato B, MMS 19	Rapporto che dovrà illustrare il processo di individuazione dei rischi, evidenziando le modalità di individuazione di tutti gli elementi/variabili di determinazione del rischio (classificazione dei dati personali in comuni / sensibili/giudiziari, probabilità di accadimento delle minacce, livello di vulnerabilità dei sistemi informatici) e la relazione esistente fra queste variabili che determinano il livello di rischio esistente.



Attività di Verifica	Ambiente informatico interessato	Frequenza	Rif. Testo Unico Privacy	Evidenza oggettiva dell'attività
				Tale rapporto e la relativa metodologia di analisi dei rischi sono normalmente riportati all'interno del Documento Programmatico sulla Sicurezza, in una apposita sezione dedicata alla tematica dell'analisi dei rischi.
Analisi e valutazione delle minacce e vulnerabilità tecnologiche.	Personal computer nella LAN di Milano. Piattaforma AS400	Semestrale	Allegato B, MMS 17	Rapporto per la valutazione delle vulnerabilità di sicurezza predisposto tramite l'utilizzo di tool automatici o tramite esecuzione di programmi di lavoro (check-list di controlli di sicurezza /controlli IT), a seconda dell'ambiente informatico interessato.
Tenuta e revisione del corpo documentale delle procedure privacy (es. atti di nomina, informative, procedure di sicurezza dei dati, regolamento utente)	Tutti i sistemi informatici che supportano il trattamento di dati personali.	Ad- Hoc, in conseguenza di eventuale evoluzione organizzativa interna o di evoluzione dei sistemi informativi.	Allegato B, MMS 4, 9, 18, 21, 27	Aggiornamento dell'archivio centrale presente alla sede di Milano, e contenente tutti gli atti di nomina a responsabile e ad incaricato del trattamento e la relativa modulistica privacy (modelli documentali).



<i>Attività di Verifica</i>	<i>Ambiente informatico interessato</i>	<i>Frequenza</i>	<i>Rif. Testo Unico Privacy</i>	<i>Evidenza oggettiva dell'attività</i>
		Per le procedure o policy che verranno eventualmente emanate in futuro, le modalità e i tempi di revisione saranno determinati successivamente alla loro prima predisposizione.		
Revisione delle utenze e profili informatici	Applicazioni su AS400	Annuale	Allegato B, MMS 14	<p>Rapporto di revisione periodica dei profili utente:</p> <ul style="list-style-type: none"> ▪ La data dell'avvenuta operazione di revisione, ▪ L'autore della revisione, ▪ Le utenze verificate e i sistemi target oggetto di revisione ▪ Le eventuali anomalie riscontrate, ▪ Le eventuali osservazioni o raccomandazioni,



<i>Attività di Verifica</i>	<i>Ambiente informatico interessato</i>	<i>Frequenza</i>	<i>Rif. Testo Unico Privacy</i>	<i>Evidenza oggettiva dell'attività</i>
Verifica del buon esito della procedura di backup	AS400	Giornaliero	Allegato B, MMS 18	Calendario di schedulazione del backup e log di buon esito del backup.
Verifica dell'effettiva installazione/applicazione su sistemi e applicazioni degli aggiornamenti correttivi per le vulnerabilità e i difetti riconosciuti (antivirus, update di patch di sistema e/o di sicurezza)	Personal computer	Il controllo è previsto trimestrale, o ad hoc su eventuali necessità.	Allegato B, MMS 17	Schermata che comprova regolare aggiornamento dell'antivirus e delle patch di sistema.

Tabella 7. *Programma di revisione e monitoraggio periodico delle Misure Minime di Sicurezza*

13 Modulistica

Mpr-01	Censimento postazioni di lavoro
Mpr-02	Censimento dei trattamenti elettronici e cartacei
Mpr-03/01	Nomina del responsabile interno del trattamento dati
Mpr-03/02	Nomina del responsabile esterno del trattamento dati
Mpr-04/01	Nomina incaricati interni del trattamento dati
Mpr-04/02	Nomina incaricati esterni del trattamento dati
Mpr-05	Elenco responsabili e incaricati
Mpr-06	Firme per accettazione incarichi collettivi

Appendice

Riferimento legislativo

Per scopi divulgativi si riporta a seguire una breve presentazione delle principali disposizioni della normativa vigente in Italia in tema di Privacy (il D.lgs. 196/2003, denominato anche Testo Unico sulla Privacy), che è stata presa in considerazione per la stesura del presente documento.

Adozione di misure di sicurezza

Art.31 (Sicurezza dei dati): *‘i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l’adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o non consentito o non conforme alla finalità della raccolta’.* (comma 1).

Responsabilità civile

L’art.15 del T.U. (Danni cagionati per effetto del trattamento dei dati personali) prevede che chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell’art.2050 del codice civile.

Il danno non patrimoniale è risarcibile anche in caso di violazione dei principi previsti dall’art.11 del T.U., in tema di trattamento dei dati personali: *...ossia i dati personali oggetto di trattamento devono essere:*

- *trattati in modo lecito e secondo correttezza;*
- *raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;*
- *esatti e, se necessario, aggiornati;*
- *pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;*
- *conservati in una forma che consenta l’identificazione dell’interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.*

Adozione di misure minime di sicurezza

Per “misure minime” si intende il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall’art. 31 del T.U.

L’Art 33 del T.U. prevede l’obbligo di adozione di tali misure minime di sicurezza e gli articoli 34 e 35 del T.U. individuano le tipologie di misure minime di sicurezza da adottare. I criteri e le modalità di adozione di tali misure sono espressi nel Disciplinare Tecnico (allegato B del T.U.).

Nella tabella a seguire si riportano in dettaglio le suddette modalità di adozione delle misure minime di sicurezza.



ID Misura Minima	Riferimento Articolo del Testo Unico	Descrizione
MM1	Art. 34 a), b)	Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
MM2		Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
MM3		Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
MM4		Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
MM5		La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
MM6		Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
MM7		Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
MM8		Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
MM9		Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
MM10		Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
MM11		Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.



ID Misura Minima	Riferimento Articolo del Testo Unico	Descrizione
MM12	Art. 34 c)	Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
MM13		I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
MM14		Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
MM15	Art.34 d) e) f)	Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
MM16		I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615- <i>quinquies</i> del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
MM17		Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
MM18		Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
MM19	Art. 34 g)	<p>Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:</p> <p>19.1. l'elenco dei trattamenti di dati personali;</p> <p>19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;</p> <p>19.3. l'analisi dei rischi che incombono sui dati;</p> <p>19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;</p> <p>19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;</p> <p>19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;</p> <p>19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati</p>



ID Misura Minima	Riferimento Articolo del Testo Unico	Descrizione
		<p>personali affidati, in conformità al codice, all'esterno della struttura del titolare;</p> <p>19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.</p>
MM20	Art.34 e) f) h)	I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-terdel codice penale, mediante l'utilizzo di idonei strumenti elettronici.
MM21		Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
MM22		I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
MM23		Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
MM24		Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.
MM25	Disciplinare Tecnico Allegato B) al Testo Unico	Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
MM26		Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
MM27	Art. 35 b), c), e Disciplinare Tecnico, punti 27, 28 e 29.	Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.



ID Misura Minima	Riferimento Articolo del Testo Unico	Descrizione
MM28		Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
MM29		L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Adozione di misure e accorgimenti relativamente alle attribuzioni delle funzioni di amministratore di sistema

L'Autorità Garante per la Privacy ha emanato il 27 novembre 2008 un Provvedimento, le cui prescrizioni del presente si applicano a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 della legge 133/2008, di conversione del decreto-legge 112/2008, laddove si riferisce ai soggetti che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese).

A seguire si riportano in sintesi le misure previste in tema di attribuzione delle funzioni di amministratore di sistema:

a) Valutazione delle caratteristiche soggettive.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

b) Designazioni individuali.

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c) Elenco degli amministratori di sistema.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante).

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano dati personali dei lavoratori, i titolari sono tenuti a rendere nota l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni. Ciò avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del codice privacy nell'ambito del



rapporto di lavoro, oppure tramite il disciplinare tecnico di cui al Provvedimento del Garante del 1° marzo 2007 (linee guida per posta elettronica e internet nell'ambito del rapporto di lavoro) o, in alternativa, mediante altri strumenti di comunicazione interna (ad esempio intranet aziendale, ordini di servizio a circolazione interna o bollettini).

d) Servizi in outsourcing.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno del trattamento deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e) Verifica delle attività.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f) Registrazione degli accessi.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Responsabilità penale:

Oltre ad una responsabilità civile, è prevista dall'art. 169 del T.U. una responsabilità penale, in caso di omessa adozione delle misure minime di sicurezza. E' prevista la sanzione penale della reclusione fino a 2 anni o l'ammenda da diecimila euro a cinquantamila euro.

Predisposizione del Documento Programmatico Sulla Sicurezza (DPS):

L'art. 34 comma g) prevede l'obbligo di predisposizione del DPS, in caso di trattamento dei dati personali effettuato con strumenti elettronici.

Secondo quanto previsto dal Disciplinare Tecnico del Testo Unico, recante i criteri e le modalità di adozione delle misure minime di sicurezza, il DPS, previsto nel caso di trattamento dei dati sensibili e/o giudiziari, dovrebbe essere aggiornato entro il 31 marzo di ogni anno e contenere informazioni in merito a:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati sensibili o giudiziari in seguito a distruzione o danneggiamento, in tempi certi



compatibili con i diritti degli interessati e non superiori a sette giorni. (punto 19.5 e punto 23);

- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale, trattati da organismi sanitari o esercenti le professioni sanitarie, dagli altri dati personali dell'interessato (pti 19.8, 23).