REGIONE PIEMONTE

AZIENDA SANITARIA LOCALE VCO

OMEGNA

IL DIRETTORE GENERALE

DELIBERAZIONE N. 357 del 14 OTTOBRE 2015

OGGETTO	**AGGIORNAMENTO DEL MANUALE DI GESTIONE DEL SISTEMA INFORMATIVO DI PROTOCOLLO E DI GESTIONE DOCUMENTALE**

L'anno duemilaquindici il giorno QUATTORDICI

del mese di OTTOBRE in OMEGNA,

IL DIRETTORE GENERALE

- Dott. Giovanni Caruso

coadiuvato da:

- Dott. Antonino Trimarchi DIRETTORE SANITARIO

- Dott. Antonio Jannelli DIRETTORE AMMINISTRATIVO

Riservato alla S.O.C. Gestione delle Risorse Economiche e Finanziarie per la registrazione della spesa
data _____

al N. _____ conto _____

al N. _____ conto _____

al N. _____ conto _____

al N. _____ conto _____

Si attesta la regolarità contabile e le imputazioni a Bilancio derivanti dal provvedimento
Il Direttore F.F. SOC REF
(Dott.ssa Manuela Succi)

_____

Beneficiario _____ €. _____

Beneficiario _____ €. _____

Beneficiario _____ €. _____

Annotazioni eventuali :

357 14 OTTOBRE 2015

PROPOSTA ISTRUTTORIA
IL DIRETTORE SOC AFFARI GENERALI

RICHIAMATE le vigenti disposizioni normative e regolamentari in materia di protocollo informatico, dei flussi documentali ed in particolare:

- il D.P.C.M. 31 ottobre 2000 recante " Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998 n. 428";
- il D.P.R. 28 dicembre 2000 n. 445 recante "il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- la direttiva del Ministero per l'innovazione e le tecnologie del 9 dicembre 2002, avente per oggetto "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali";
- il D.Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati pesonali";
- il Decreto del Ministero per l'Innovazione e le Tecnologie del 14 ottobre 2003, recante approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei documenti amministrativi;
- il D.Lgs. 7 marzo 2005 n. 82 e s.m.i. di approvazione del Codice dell'Amministrazione Digitale
- il D.P.C.M. 13 novembre 2014 recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 *-bis* , 23 *-ter* , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

RICHIAMATE altresì

- la deliberazione aziendale n. 537 del 30/12/2003 avente per oggetto il Manuale di gestione del protocollo informatico;
- la deliberazione aziendale n. 78 del 2 febbraio 2006 con la quale è stato approvato un primo aggiornamento del Manuale di Gestione del Protocollo informatico dell'ASL VCO in applicazione alle disposizioni di legge;
- la deliberazione aziendale n. 967 del 31/12/2009 con la quale è stato approvato un secondo aggiornamento del Manuale di Gestione del Protocollo Informatico dell'ASL VCO al fine garantire un'armonizzazione con le nuove disposizioni;
- la deliberazione aziendale n. 487 del 22/12/2014 con il quale è stato approvato un terzo aggiornamento del Manuale di gestione del sistema informativo di protocollo

PRESO ATTO che risulta necessario provvedere, sia per intervenute modificazioni organizzative interne che per adeguare le procedure alle vigenti disposizioni, ad aggiornare il Manuale di Gestione del Sistema Informativo di Protocollo e di gestione documentale dell'ASL VCO

Ritenuto di dover pertanto procedere alla formale approvazione del manuale aggiornato, che viene allegato alla presente deliberazione sotto la lettera A) e che determina contestualmente la cessazione degli effetti di quanto disposto con precedente deliberazione n. 487 del 22/12/2014

PROPONE DI DELIBERARE

1°) di provvedere, per le motivazioni citate in premesse ed ivi tutte richiamate, all'aggiornamento del Manuale di Gestione del Sistema Informativo di Protocollo e di gestione documentale dell'ASL VCO così come da allegato a) al presente provvedimento che ne forma parte integrante e sostanziale;

2°) di dare atto che l'allegato a) al presente provvedimento va a sostituire l'allegato a) alla deliberazione n. 487 del 22/12/2014;

3°) di disporre, al fine di dare avvio alla rivisitazione del titolario di classificazione e del massimario di scarto nonché alla valutazione di tutte le fasi e le azioni da intraprendere per dare compiuta applicazione alle disposizioni del Codice dell'Amministrazione digitale in tema di "documento informatico" e gestione documentale così come previsto all'art. 1.5, la costituzione di un apposito gruppo di lavoro così costituito:

DIRETTORE SOC AFFARI GENERALI	Dr.ssa Anna Rosa Bellotti
DIRETTORE DIP. TECNICO AMMINISTRATIVO	Dr. Federico Bonisoli
RESPONSABILE AZIENDALE DELLA TRASPARENZA	Dr.ssa Pimatesta Giuseppina
DIRETTORE SOC INFORMATION COMUNICATION TECNOLOGY	Dr.ssa Anna Gagliardi
RESPONSABILE AZIENDALE ANTICORRUZIONE	Dr. Luigi Petrone

4°) di provvedere alla pubblicazione del presente Manuale sul sito INTERNET ed INTRANET aziendale al fine di consentirne la massima diffusione.

5°) di disporre l'immediata esecutività del presente provvedimento in considerazione dell'urgenza di dar corso alle disposizioni ivi contenute.

Si attesta la regolarità tecnica e la legittimità del provvedimento proposto

Il Direttore SOC Affari Generali
Responsabile del Procedimento
(Dott.ssa Anna Rosa Bellotti)

IL DIRETTORE GENERALE

VISTA la sopraestesa proposta istruttoria

ACQUISITI i pareri favorevoli espressi, ai sensi dell'art. 3, comma 1-quinquies, del D.lgs. n . 229/1999 dal Direttore Amministrativo e dal Direttore Sanitario

DECIDE

di approvarla integralmente adottandola quale propria deliberazione.

Letto, confermato e sottoscritto

IL DIRETTORE GENERALE
(Dott. Giovanni Caruso)

IL DIRETTORE SANITARIO
(Dott. Antonino Trimarchi)

IL DIRETTORE AMMINISTRATIVO
(Dott. Antonio Jannelli)

RELAZIONE DI PUBBLICAZIONE

Si attesta che copia del presente atto è stata posta in pubblicazione all'Albo Ufficiale dell' A.S.L. VCO il giorno 14 OTT. 2015 per 15 giorni continuativi.

IL FUNZIONARIO INCARICATO

IMMEDIATAMENTE ESECUTIVA

~~ESECUTIVITA'~~ IN DATA 14 OTT. 2015

IL FUNZIONARIO INCARICATO
L'Assistente Amministrativo
(Laura [illegible])

Trasmissione a:

- Collegio Sindacale — Nota prot. n. _____ del _____
- Conferenza dei Sindaci — Nota prot. n. _____ del _____
- Giunta Regionale — Nota prot. n. _____ del _____

Copia per strutture:

☐ DSO V	☐ DSM	☐ MED. COMP	☐ DIP. EMERG. URG.
☐ SERT	☐ DP	☐ FE	☐ DIP. AREA CRITICA
☐ DIST. 0	☐ F	☐ REF	☐ DIP. DIPENDENZE
☐ DIST. V	☐ SD	☐ ITB	☐ DIP. POST ACUZIE
☐ DIST. D	☐ LP	☐ ICT	☐ DIP. PAT. CNV
☐ ML	☐ AG	☐ DIP. PAT. CHIRUR.	☐ DIP. FARMACO
☐ MED URG	☐ BC	☐ DIP TECNICO AMMVO	☐ DIP. PAT. MEDICHE
☐ SITRPO	☐ RU	☐ DIP. PAT. ONCOL.	☐ DIP. MAT. INF.
☐	☐ PP	☐ DIP. SERVIZI DIAGN.	☐ PSICOLOGIA
☐	☐	☐	☐

ALLEGATO A) ALLA DELIBERAZIONE N. 357 DEL 14 OTTOBRE 2015

MANUALE DI GESTIONE DEL SISTEMA INFORMATIVO DI PROTOCOLLO E DI GESTIONE DOCUMENTALE ASL V.C.O. "Aggiornamento 2015"

Parte Prima

Introduzione e atti preliminari

1. Che cos'è, a cosa e a chi serve questo Manuale

Entro il 31 dicembre 2003 tutte le pubbliche amministrazioni hanno dovuto introdurre il protocollo Informatico, secondo quanto stabilito dal pacchetto normativo collegato alla Bassanini 1 (legge 15 marzo 1997, n. 59), confluito per lo più nel DPR 28 dicembre 2000, n. 445, recante il *Testo unico sulla documentazione amministrativa.*

L'art. 5 del DPCM 31 ottobre 2000, contenente le *Regole tecniche sul protocollo informatico*, ha previsto inoltre che le pubbliche amministrazioni redigano un *Manuale* per la gestione del protocollo, dei flussi documentali e degli archivi rivisto ed integrato dal Codice dell'Amministrazione Digitale.

Si trattava di uno strumento operativo che, per il grado di analisi che ogni amministrazione è chiamata ad effettuare, può rappresentare un primo e significativo passo verso la certificazione di qualità del servizio.

Il dettato del DPCM 31 ottobre 2000 e s.m.i. e le vigenti disposizioni CAD (codice dell'Amministrazione Digitale) hanno previsto infatti che il *Manuale* affronti alcuni aspetti cruciali, quali la gestione e la tenuta del protocollo informatico e dei documenti su vari supporti, la migrazione dei documenti informatici, l'introduzione dei titolari di classificazione e dei massimari di selezione, nonché la definizione delle linee strategiche legate al *recordkeeping system* (cioè al sistema archivistico) e al *workflow management* (cioè al sistema di flusso di lavoro e delle procedure ad esso collegate).

Questo quarto aggiornamento del *Manuale* è adottato ai sensi dell'art. 3 comma 1 lettera d) del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante le regole tecniche per il protocollo informatico. Il manuale, ai sensi dell'art. 5 comma 1 "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

E' rivolto ai dirigenti, ai quadri e agli operatori di protocollo e della gestione del flusso documentale dell'A.S.L. V.C.O., come strumento di lavoro per la gestione dei documenti, degli affari e dei procedimenti amministrativi che sono chiamati a trattare e dei quali sono individuati come responsabili.

Il *Manuale* descrive le fasi operative del sistema per la gestione del protocollo informatico, dei flussi documentali e degli archivi, individuando azioni e processi amministrativi con i livelli di esecuzione, responsabilità e controllo, in una visione d'insieme – senza soluzioni di continuità – dal

protocollo all'archivio storico. La normativa a supporto del presente manuale è contenuta **nell'allegato 1.**

1.1 Atti di organizzazione preliminari

L'entrata in vigore del protocollo unico è stata preceduta dall'adozione di specifici atti di organizzazione, così come previsto dal decreto legislativo 3 febbraio 1993, n. 29 (e successive modificazioni) e in armonia con le disposizioni già previste dal DPR 20 ottobre 1998, n. 428 (oggi confluito nel DPR 445/2000).
Tali atti di organizzazione sono stati i seguenti:
a) individuazione delle Aree Organizzative Omogenee (AOO) dell'A.S.L. V.C.O. nelle quali adottare il protocollo unico;
b) individuazione delle Unità Organizzative Responsabili (UOR) in cui è articolata ciascuna AOO e che afferiscono al protocollo unico;
c) introduzione del protocollo unico ed eliminazione dei protocolli interni;

1.2 Individuazione dell'Area organizzativa omogenea (AOO)

L'AZIENDA SANITARIA LOCALE viene considerata **unica area organizzativa omogenea**, con **codice I.P.A asl14_vco** così come d'altro canto contenuto nelle indicazione dettate dalla Sovrintendenza Archivistica competente per territorio con nota del 13/08/2003 pervenuta in data 26/08/2003 prot. 27998/03.
Pertanto l'Azienda Sanitaria V.C.O. è dotata di un protocollo unico e le strutture presenti in Azienda e sotto riportate sono state individuate quali Unità Organizzative Responsabili in rete sul sistema di protocollo integrato aziendale .

CODICE	SIGLA	STRUTTURA
01	DSO	OSPEDALE UNICO PLURISEDE
02	DP	DIPARTIMENTO PREVENZIONE
03	DIST O	DISTRETTO OMEGNA
04	DIST V	DISTRETTO VERBANIA
05	DIST D	DISTRETTO DOMODOSSOLA
07	ML	MEDICINA LEGALE
08	SERT	SERT
09	DSM	DIPARTIMENTO SALUTE MENTALE
10	ASA	ASSISTENZA SPECIALISTICA AMBULATORIALE
11	ES	EDUCAZIONE SALUTE
12	F	FARMACIA
13	SD DU	DIPLOMI UNIVERSITARI
14	NPI	NEUROPSICHIATRIA INFANTILE
15	DSO DMI	DIPARTIMENTO MATERNO INFANTILE
18	SD	SUPPORTO DIREZIONALE
20	AG	AFFARI GENERALI
21	ALP	AFFARI LEGALI E PATRIMONIALI
22	BC	BUDGET E CONTROLLO
24	FL	FORNITURE E LOGISTICA
25	ITB	INFRASTRUTTURE TECNOLOGIE BIOMEDICHE
26	PP	PREVENZIONE PROTEZIONE
27	MC	MEDICO COMPETENTE
28	COLL SIND	COLLEGIO SINDACALE
29	CONS SAN	CONSIGLIO SANITARI

30	DG	DIREZIONE GENERALE
31	ICT	TECNOL. INFORMATICHE E SIST. INFORMATIVO
33	RAP SIND	RAPPRESENTANZA SINDACI
34	REF	RISORSE ECONOMICO FINANZIARIE
35	SD OIV	ORGANISMO INDIPENDENTE DI VALUTAZIONE
38	MCU	MEDICINA CHIRURGIA URGENZA
41	DSO DPC	DIPARTIMENTO PATOLOGIE CHIRURGICHE
42	DSO DPM	DIPARTIMENTO PATOLOGIE MEDICA
43	DSO DEU	DIPARTIMENTO EMERGENZA URGENZA
46	F CTFV	COMMIS. TECNICA FARMACEUTICA VIGILANZA
47	DSO UPRI	UNITA' PREVENZIONE RISCHIO INFETTIVO
48	DSM PSIC	SERVIZIO PSICOLOGIA
49	SPV	SERVIZI VETERINARI
50	SIAN	SIAN
51	SISP	SERVIZIO IGIENE SANITA' PUBBLICA SISP
52	SPRESAL	SERVIZIO PREVENZIONE SICUREZZA AMBIENTI LAVORO
57	SITRPO	SERVIZIO INFERM. TECNICO RIABILIT. PREV. OSTETRICA
58	FS	FISICA SANITARIA
59	DSO DSD	DIPARTIMENTO SERV. DIAGNOST. SUPPORTO
60	DSO DNCV	DIPARTIMENTO CARDIONEUROVASCOLARE
61	DSO DPA	DIPARTIMENTO POST ACUZIE
62	DSO DAC	DIPARTIMENTO AREA CRITICA
63	DSO DPO	DIPARTIMENTO PATOLOGIE ONCOLOGICHE
64	EPI	EPIDEMIOLOGIA
66	RU	RISORSE UMANE
67	CONF PART	CONFERENZA PARTECIPAZIONE
68		SEGRETERIA DIP. TECNICO AMMINISTRATIVO
69	RLS	RAPPRESENTANTI PER LA SICUREZZA
70	SS	SERVIZIO SOCIALE
71	CZ	COMITATO ZONALE
72	SI	SERVIZIO ISPETTIVO
73	CP	CURE PALLIATIVE
74	CUG	COMITATO UNICO GARANZIA
75	QA	QUALITA' ACCREDITAMENTO
76		UFFICIO ANAGRAFE SANITARIA
77		COORDINATORE AMMINISTRATIVO
78	RT	RESPONSABILE AZIENDALE TRASPARENZA
79	RC	RESPONSABILE PREVENZIONE DELLA CORRUZIONE
99		TUTTI I SERVIZI

1.3 Individuazione del servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi

Nell'A.S.L. V.C.O. è stato istituito un servizio avente il compito di gestire il protocollo informatico e coordinare i flussi documentali informatici correlati. Gli archivi cartacei permangono ancora sotto la piena responsabilità dei Direttori di Dipartimento, dei Direttori di Struttura Complessa e dei Responsabili di struttura semplice dipartimentale o loro delegati.

Al fine di garantire normalizzazione ed economia di scala, **il Responsabile del Servizio di Protocollo Informatico e della gestione documentale amministrativa informatica correlata alla procedura ARCHIFLOW risulta anche il Responsabile della Struttura Organizzativa Complessa di Gestione degli Affari Generali** che ha provveduto, sin dal 2003, all'avvio della

procedura di aggiornamento del sistema del protocollo, ed ha garantito il costante aggiornamento, con i Responsabili di struttura, del personale da abilitarsi per l'accesso alla procedura gestionale (provvedendo al continuo aggiornamento delle abilitazioni e disabilitazioni) e *garantendo la formazione di tale personale.* **Ai sensi delle vigenti disposizioni del CAD il dirigente vicario risulta il Direttore del Dipartimento dei Servizi tecnico Amministrativi e di supporto direzionale.**

1.4 Introduzione del protocollo unico ed eliminazione dei protocolli interni

Con l'entrata in vigore del protocollo unico, sin dal 2003, sono cessati di diritto tutti i cosiddetti protocolli interni (cioè di struttura complessa, protocolli multipli, protocollo del telefax, etc.) o altri sistemi di registrazione o registratura dei documenti diversi dal protocollo unico. Il responsabile del servizio di protocollo effettua controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale, e sull'utilizzo di un unico registro informatico.

1.5 Titolario di classificazione

Con l'entrata in vigore del protocollo unico (anno 2003) si era addivenuti alla realizzazione ed approvazione da parte della Sopraintendenza archivistica di un Titolario unico di classificazione. Si trattava di un sistema logico che suddivideva però i documenti secondo la funzione esercitata in ogni struttura. Stante la complessità del sistema e l'esigenza di adeguamenti tecnologici con la contestuale necessità di risorse umane da formarsi è stata rimandata e poi definitivamente sospesa la fase sperimentale di attuazione. Oggi risulta indispensabile rivedere sostanzialmente tale titolario alla luce delle intervenute modificazioni delle strutture aziendali e delle funzioni ad esse attribuite.
Verrà avviata pertanto una completa revisione sia del titolario di classificazione che un aggiornamento del massimario di conservazione e scarto per consentire a tutti gli operatori di avere piena consapevolezza dell'importanza dell'archivio e della conservazione dei documenti, sia cartacei che informatici, nel rispetto delle vigenti disposizioni.
La Direzione Generale provvederà pertanto alla costituzione di un Gruppo di Lavoro che sarà finalizzato alla definizione del nuovo titolario di classificazione ed alla revisione del massimario di conservazione e scarto nonché alla valutazione di tutte le fasi e le azioni da intraprendere per dare compiuta applicazione alle disposizioni del Codice dell'Amministrazione digitale in tema di "documento informatico" e gestione documentale.

1.6 Massimario di selezione

Il prontuario di selezione contiene l'elenco delle tipologie documentali con l'indicazione del tempo di conservazione . L'utilizzo del Massimario, ad avvenuto perfezionamento dell'iter procedurale correlato al parere della Sopraintendenza Archivistica , sarà comunicato con atto del Direttore Generale.

Parte Seconda

Il documento

2.A FORMAZIONE DEI DOCUMENTI

2.A1 Il documento amministrativo

Per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, informatica o di qualsiasi altra specie del contenuto di atti, fatti o cose giuridicamente rilevanti, anche interni, prodotti e acquisiti ai fini dell'attività amministrativa, così come prevede l'art. 22 comma 2 della legge 7 agosto 1990, n. 241 e s.m.i.

Un documento amministrativo è dunque una rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa come previsto dall'art. 1 comma 1, lettera a D.P.R. 445/2000.

2.A2. Il documento informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti ai sensi dell'art. 1 lettera p) del D.Lgs. n. 82/2005 ed a tale proposito con Decreto del Presidente del Consiglio dei Ministri del 13/11/2014 sono state definite le regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni.

I documenti informatici prodotti dall'Azienda quali rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti ai sensi dell'art. 1, lett. p) del CAD, indipendentemente dal *software* utilizzato, prima della loro sottoscrizione con firma elettronico/digitale, saranno convertiti in uno dei formati *standard* previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione, nonché l'immutabilità nel tempo del contenuto e della struttura, come previsto dal Piano di continuità operativa (**allegato 2**) e dalle norme vigenti in tema di conservazione sostitutiva.

2.A3 Modalità di formazione dei documenti e contenuti minimi

Le modalità di formazione dei documenti, la loro struttura, il loro formato e gli altri elementi base sono determinati dalla Direzione Aziendale e da quanto previsto dal presente Manuale. Per quanto riguarda i documenti informatici, le deliberazioni, le determinazioni e le lettere la loro produzione è regolata sulla base di modelli standard che saranno pubblicati sul sistema intranet aziendale .

Il contenuto minimo di ciascun documento deve comunque garantire la presenza delle seguenti informazioni:

- denominazione e logo dell'Azienda (per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto dall'Azienda);
- indicazione della struttura aziendale che ha prodotto il documento;
- indirizzo e recapiti completi (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica dell'Azienda);
- data: luogo, giorno, mese, anno;
- destinatario/i per competenza e conoscenza;
- oggetto del documento, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- classificazione (titolo, categoria, classe, sottoclasse e fascicolo) da inserire al momento dell'approvazione del titolario di classificazione aziendale;
- numero degli allegati e breve descrizione, se presenti;
- numero di protocollo;

- testo;
- sottoscrizione autografa o elettronico/digitale del Dirigente Responsabile (o del funzionario delegato);
- indicazione del Responsabile del procedimento (Legge 7 agosto 1990, n. 241 e ss. mm. e ii.);
- indicazione dello scrittore /referente per la pratica (sigle).

2.A4 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge.

Per quanto concerne la firma digitale, l'Azienda si avvale dei servizi di certificazione offerti da INFOCERT iscritta nell'elenco dei certificatori di cui all'art. 8 del DPR 513/2007.

2.A5 Valore probatorio del documento informatico

Ai sensi dell'art. 20, c. 1-bis del CAD, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento stesso.

Laddove sottoscritto, il documento informatico ha il valore probatorio di cui all'art. 21 del CAD:

"*1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.*

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

2-bis Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione Europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nell'Unione Europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione Europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie".

2.A6 Documenti cartacei: originali, minute e copie .

Per ogni documento cartaceo destinato ad essere spedito in originale vengono scritti tanti esemplari quanti sono i destinatari ESTERNI all'azienda e tanti quanti sono i destinatari per competenza interni all'azienda. La posta per conoscenza ai destinatari interni deve essere letta giornalmente attraverso il sistema di gestione documentale che consente di registrare traccia permanente dell'avvenuta lettura e non deve essere inviata una copia cartacea. *Si precisa sin da ora che ad avvenuta assegnazione della firma digitale le strutture aziendali trasmetteranno la posta interna solamente tramite l'applicativo gestionale ARCHIFLOW (tra le strutture in rete) e attraverso mail aziendale agli altri destinatari interni.*

L'originale rappresenta la redazione definitiva, perfetta e autentica negli elementi sostanziali e formali.

La minuta cartacea rappresenta la redazione definitiva del documento da conservare "agli atti". Essa porta la firma autografa ed è conservata nel fascicolo del procedimento al quale si riferisce o nell'apposita serie documentaria. Anche sulla minuta è apposta la segnatura di protocollo a cura della struttura emittente.

Qualora si renda necessario, per ragioni amministrative, si possono produrre copie di un medesimo documento. Su ciascuna copia va apposta la dicitura "copia" a cura della struttura.

Le copie trasmesse per ragioni amministrative ad altre strutture organizzative sono conservate da queste ultime per tutto il tempo necessario allo svolgimento del procedimento cui il documento si riferisce e quindi eliminate secondo le norme che saranno previste nel massimario di scarto in fase di revisione.

Per quanto riguarda il regime giuridico delle copie informatiche di documento analogico/cartaceo si rimanda agli articoli 23-ter c. 3 del CAD (copie informatiche di documenti formati in origine su supporto analogico, da intendersi quale *"documento informatico avente contenuto identico a quello del documento da cui è tratto")* e all'art. 22 c. 2 del CAD (copie per immagine su supporto informatico di documento analogico, da intendersi quale *"documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto"*):

- art. 23–ter c. 3 del CAD, le copie informatiche di documenti formati in origine su supporto analogico "*hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato (...) mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche*" vigenti in materia.

In assenza della predetta attestazione di conformità, si applica il regime probatorio generale di cui all'art. 2719 c.c. (secondo il quale le copie hanno medesima efficacia degli originali, salvo espresso disconoscimento).

- art. 22 c. 2 del CAD, le copie per immagine su supporto informatico di documenti originali analogici "*hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche*" vigenti in materia.

In assenza della predetta attestazione di conformità, l'art. 22 c.3 prevede che esse abbiano la stessa efficacia probatoria degli originali "*se la loro conformità all'originale non è espressamente disconosciuta*".

2.A7 Tutela della riservatezza

I documenti, le banche dati, il protocollo e gli altri registri, sono prodotti in modo da tutelare la riservatezza dei dati personali, dei dati sensibili e dei dati giudiziari ai sensi della normativa vigente Tutti gli operatori che accedono a vario titolo devono essere formalmente individuati quali "incaricati al trattamento " dal proprio Responsabile così come previsto peraltro nel vigente Manuale aziendale per la sicurezza del trattamento dei dati personali di cui alla deliberazione n. 738 del 15/12/2005. La graduazione dell'accesso al sistema documentale informatico ARCHIFLOW da

parte degli operatori è definito da ogni responsabile di struttura e deve rispettare il criterio di non eccedenza al trattamento come previsto dalle vigenti disposizioni del Garante Privacy.

2.B.TIPOLOGIA DEI DOCUMENTI AZIENDALI

I documenti si distinguono in documenti in arrivo dall'esterno, documenti in partenza verso l'esterno, e documenti interni in arrivo e partenza da e verso strutture interne.

2.B1 Documenti in arrivo

Per documenti in arrivo si intendono i documenti che hanno rilevanza giuridico-probatoria, acquisiti dall'AOO nell'esercizio delle proprie funzioni.

2.B2 Ricezione dei documenti su supporto cartaceo

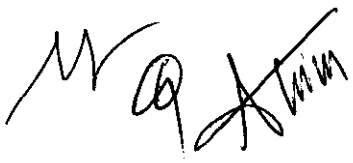
I documenti su supporto cartaceo possono pervenire all'Area Organizzativa Omogenea, presso la sede dell'Ufficio protocollo Aziendale attraverso una delle seguenti modalità:
a) posta (ordinaria, raccomandata, celere, corriere espresso, ecc. sistema lotus regionale);
b) fax;
c) consegna diretta *brevi manu*;
d) servizio di collegamento interno con automezzi aziendali

I documenti pervenuti via fax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei; in presenza di un sistema informatico che ne consente l'acquisizione in formato elettronico (fax *management*) si applicano le procedure previste per la ricezione dei documenti informatici

L'operazione di segnatura per i documenti IN ARRIVO DALL'ESTERNO è di norma effettuata centralmente presso il PROTOCOLLO GENERALE fatte salve le eccezioni di cui **all'allegato 3.**
I documenti registrati vengono poi smistati alla o alle STRUTTURE di competenza (di norma una sola) che procede all'individuazione del Responsabile Procedimento Amministrativo; il RPA è incaricato delle successive operazioni di classificazione (che dovranno avvenire entro tre giorni dall'assegnazione), di fascicolazione e di archiviazione; vale a dire della corretta creazione e gestione del fascicolo relativo all'affare o al procedimento amministrativo in questione (sia cartaceo che informatico). Qualora non è individuato il RPA tale responsabilità ricade sul Direttore della Struttura stessa.
Nel caso di notifica di atti giudiziari nominativi o indirizzati a direttori di struttura (indicazione della funzione) provenienti dal Tribunale al protocollo generale, sarà cura dell'ufficio protocollo apporre la protocollazione sulla busta chiusa con individuazione della competenza nominativa e l'inserimento per conoscenza degli Affari Generali. Il Responsabile della SOC Affari Generali provvederà a comunicare per iscritto all'interessato, che è giacente presso il Protocollo Generale la comunicazione citata affinché venga ritirata entro tre giorni lavorativi. Ad avvenuto ritiro da parte dell'interessato o di suo delegato (delega formale per iscritto) sarà richiesta l'apposizione di firma e data per ricevuta ed il personale del protocollo effettuerà una aggiuntiva scansione del modulo di avvenuta consegna.
Tutte le altre notifiche di atti giudiziari (provenienti per esempio da Avvocati ecc...) o indirizzati genericamente all'Avvocato Cinzia meloda (incaricato alla difesa dell'Azienda) o all'ASL VCO o genericamente al LEGALE RAPPRESENTANTE DELL'ASL VCO verranno aperti dagli operatori di protocollo per la protocollazione e l'individuazione della struttura competente.

2.B3 Ricezione dei documenti informatici

I documenti informatici possono pervenire all'Area Organizzativa Omogenea, presso la Sede Aziendale attraverso:
a) spedizione via posta elettronica ordinaria o certificata;



b) trasmissione su supporto rimovibile (ad es.: Cd-Rom, DVD,) ;
La ricezione dei documenti informatici è assicurata tramite la casella aziendale di posta elettronica certificata (PEC) del protocollo generale protocollo@pec.aslvco.it che riceve sia posta certificata che elettronica ordinaria.
Il suddetto indirizzo è deputato alla funzione di ricezione/spedizione e risulta pubblicato sul sito dell'ASL VCO.
I documenti contabili (fatture) vengono invece trattati attraverso la casella PEC della SOC Gestione delle Risorse Economico finanziarie che risulta la seguente : gestione.fornitori@pec.aslvco.it

2.B4 Ricevute attestanti la ricezione dei documenti da rilasciarsi ad esterni e ricezione di posta raccomandata da vettori postali
La ricevuta della consegna di un documento cartaceo, laddove richiesta, è costituita dalla copia scansionata del primo foglio del documento stesso che riporta anche la copia dell'etichetta di segnatura che attesta il giorno della consegna.
Per la corrispondenza RACCOMANDATA consegnata da vettori postali, viene firmata la bolletta di consegna con timbro datario e firma dell'addetto ricevente e trattenuta una copia della bolletta stessa.

2.B5 Smistamento di competenza
I documenti ricevuti dal PROTOCOLLO GENERALE, dopo essere stati registrati , vengono smistati alle strutture competenti (Dipartimenti – con assegnazione tabellare e spedizione anche alla DSO per l'inoltro successivo qualora si tratti di dipartimento ospedaliero non collegato al sistema archiflow - e/o Strutture aziendali), individuate in base al modello delle competenze così come definito dall'organigramma presente nell'ATTO AZIENDALE.
Qualora pervengano al Protocollo Generale documenti inoltrati via e-mail o PEC (sia da esterni che reinoltrati da settori interni) il protocollo porrà la segnatura elettronica e non trasmetterà alcuna copia di documento cartaceo e sarà cura dei destinatari provvedere alla lettura informatica.
Il Dipartimento e/o la Struttura Complessa individuata quale competente è incaricato della gestione del procedimento cui il documento è relativo, compresa la tenuta del fascicolo cartaceo ed informatico archivistico.
L'individuazione del dipartimento e/o della struttura complessa viene effettuata dagli operatori del protocollo informatico in esito anche alla storia delle assegnazioni già avvenute in precedenza ed in correlazione alle funzioni attribuite alle strutture aziendali.

2.B6 Assegnazione di competenza
All'interno di ciascuna struttura complessa devono essere individuati i Responsabili di Procedimento Amministrativo (RPA), in base all'organizzazione delle competenze della suddetta così come definita dal Dirigente.
Il Responsabile della struttura complessa o semplice dipartimentale può, ai sensi dell'art 5 della legge 241/90 e s.m.i. assegnare a sé o altri la Responsabilità del procedimento o dell'affare individuando il RPA all'interno della propria struttura.
Il responsabile della struttura o il RPA se persona diversa dal responsabile di struttura devono, qualora il documento non sia di loro competenza, darne sollecita comunicazione al protocollo generale con le modalità indicate all'articolo 3.1b

2.B7 Conservazione delle buste o altri contenitori di documentazione
Le buste dei documenti pervenuti o le scatole o altri contenitori di documentazione si inoltrano agli uffici destinatari e vengono da questi conservati almeno per 24 ore; laddove necessario per espressa disposizione normativa o altrimenti ritenuto opportuno dal Responsabile dell'assetto assegnatario, gli stessi possono essere conservati per periodi più lunghi. Le buste delle

raccomandate sono anche scansionate nel sistema di gestione documentale affinchè ne resti traccia del numero della ricevuta.
Nel caso di ricezione dei documenti informatici, per esempio PEC, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico.

2.B8 Orari di apertura per il ricevimento della documentazione cartacea
L'Ufficio Protocollo Generale è aperto, per l'utenza esterna, dal lunedì al venerdì secondo il seguente orario: 8.30-16.00

2.B9 Documenti in partenza
Per documenti in partenza si intendono i documenti che hanno rilevanza giuridico-probatoria prodotti dal personale nell'esercizio delle proprie funzioni. La registratura dei documenti in partenza è effettuata dagli operatori di protocollo individuati dai Responsabili delle strutture aziendali e per i quali questi ultimi hanno fatto richiesta attraverso il sistema gestionale CREDNET.
Il RPA è comunque responsabile delle operazioni di protocollazione e creazione e della gestione del fascicolo relativo all'affare o al procedimento amministrativo di cui fa parte il documento protocollato.
I documenti prodotti, indipendentemente dal supporto o modalità di scrittura (informatica o meno), devono riportare, opportunamente evidenziate e se disponibili, le seguenti informazioni (già elencate al punto 2.A3) che potranno essere soggette a revisione ed aggiornamento da parte del Direttore della SOC AFFARI GENERALI in base anche alle disposizioni regionali riguardanti la carta intestata:
a) logo dell'A.S.L. V.C.O.
b) STRUTTURA COMPLESSA e/o DIPARTIMENTO, indicazione Responsabile con l'eventuale precisazione dell'area e del servizio di appartenenza;
c) indirizzo completo della sede legale dell'A.S.L.V.C.O. (via, numero, c.a.p., città, provincia,);
d) numero di telefono struttura complessa e/o semplice;
e) numero di fax;
f) indirizzo istituzionale di posta elettronica;
g) data completa (luogo, giorno, mese, anno);
h) numero di protocollo;
i) indice di classificazione composto da categoria, classe, sottoclasse, fascicolo e da altre eventuali suddivisioni qualora già attivati;
l) numero degli allegati;
m) descrizione sintetica degli allegati;
n) oggetto del documento;
o) indicazione del responsabile del procedimento e del Direttore della Struttura con relativa firma autografa o informatica (digitale)
p) sigle del responsabile, redattore ed estensore

Il Responsabile del procedimento amministrativo (RPA) oppure gli operatori dell'ufficio individuati quali operatori di protocollo provvedono a protocollare in partenza il documento stesso associando di norma il documento informatico o la scansione del documento alla registratura. Si ricorda nuovamente che, in applicazione al Codice Privacy ed alle vigenti disposizioni regolamentari aziendali il Responsabile della Struttura, nonché Responsabile del trattamento dei dati, deve provvedere alla nomina di incaricati al trattamento dei dati tutti gli operatori che accedono al sistema di protocollazione ARCHIFLOW.
Il documento cartaceo è prodotto in tanti esemplari, più uno, quanti sono i destinatari per competenza corredati di firma autografa. Gli originali sono inviati ai destinatari competenti ed uno di esso è trattenuto dalla struttura che ha redatto il documento stesso.

Il documento elettronico, prodotto conformemente alle norme di legge, dopo essere stato protocollato come documento in partenza, viene poi inoltrato informaticamente a cura di ogni struttura ai destinatari.

2.B10 Documenti interni

Per documenti interni si intendono i documenti scambiati tra le diverse STRUTTURE AZIENDALI.

Essi si distinguono in:

a) documenti di preminente carattere informativo;

b) documenti di preminente carattere giuridico-probatorio.

I documenti interni di preminente carattere informativo sono memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra uffici e di norma non vanno protocollati e si preferisce in tal caso l'uso della posta mail ordinaria.

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, e, come tali, devono essere protocollati secondo le disposizioni previste nelle sezioni seguenti.

La registratura dei documenti interni è affidata dal Responsabile Procedimento Amministrativo e/o agli operatori di protocollo della propria struttura. Il RPA è incaricato delle operazioni di creazione e gestione del fascicolo relativo all'affare o al procedimento amministrativo (sia cartaceo che informatico).

2.B11 Modalità di protocollazione delle comunicazioni in arrivo e partenza da e per i Direttori di struttura complessa ospedaliera (primari) e Direttori di Dipartimento Ospedalieri:

MODALITA' DI PROTOCOLLAZIONE DELLE COMUNICAZIONI IN ARRIVO ED IN PARTENZA DA E PER PRIMARI E DIRETTORI DI DIPARTIMENTO OSPEDALIERI:

RISULTA IMPORTANTE CHE I DIRETTORI DI STRUTTURA COMPLESSA OSPEDALIERI (PRIMARI), I DIRETTORI DI DIPARTIMENTO OSPEDALIERI E I DIRETTORI DI STRUTTURA SEMPLICE DIPARTIMENTALE OSPEDALIERA, NEL CASO DI COMUNICAZIONI IN PARTENZA, INDIVIDUINO CORRETTAMENTE IL DESTINATARIO PER COMPETENZA E QUELLI PER CONOSCENZA, NELLA CONSAPEVOLEZZA CHE I PROCESSI ED I PROCEDIMENTI PREVEDONO DEI RESPONSABILI PREPOSTI ALLA VALUTAZIONE DELLE PROBLEMATICHE.

1) COMUNICAZIONI IN ARRIVO DALL'ESTERNO AL PROTOCOLLO GENERALE ED INDIRIZZATE AL DIRETTORE DI DIPARTIMENTO OSPEDALIERO

Assegnazione per competenza al Dipartimento e sempre per conoscenza D.S.O. Sarà cura del protocollo generale far pervenire per posta interna la comunicazione al Direttore di Dipartimento tramite il servizio di consegna con automezzi aziendali. In caso di posta elettronica la comunicazione, dopo essere stata protocollata, verrà inviata alla casella mail nominativa aziendale del direttore di dipartimento.

1A) COMUNICAZIONI IN ARRIVO DALL'ESTERNO AL PROTOCOLLO GENERALE ED INDIRIZZATE AD UN DIRETTORE DI SOC E SOS DIPARTIMENTALE OSPEDALIERA

Assegnazione per competenza alla D.S.O. (senza aggiunta del nome del primario interessato).La D.S.O. provvederà a trasmettere il documento all'interessato.

2) COMUNICAZIONE DI UN DIRETTORE DI SOC OSPEDALIERA ,DI SOS DIPARTIMENTALE OSPEDALIERA E DI DIPARTIMENTO OSPEDALIERO VERSO L'ESTERNO.

Il firmatario dovrà sempre acquisire il numero di protocollo tramite la D.S.O. per formalizzare il documento in uscita. LA D.S.O. protocollerà la comunicazione in PARTENZA (in nome e per conto del Direttore di Dipartimento o del Direttore di SOC o SOS Dipartimentale)

(ovviamente comporterà l'indicazione del firmatario: sigla mnemonica dipartimento e cognome del Direttore di Dipartimento e la visibilità per conoscenza alla DSO ed al Dipartimento interessato; oppure cognome del Direttore SOC e/o SOS e visibilità per conoscenza DSO)

3) COMUNICAZIONI INVIATE DA DIRETTORI SOC OSPEDALIERE / SOS DIPARTIMENTALI OSPEDALIERE AI SOLI DIRETTORI DI DIPARTIMENTO *comportano SEMPRE, da parte del Direttore della SOC e/o SOS Dipartimentale mittente, l'inserimento tra i destinatari per conoscenza della D.S.O. .*

Sarà infatti la DSO a protocollare in arrivo la comunicazione individuando:
per competenza il Direttore di Dipartimento (tabellare)
e p.c. la DSO (tabellare)

3A) COMUNICAZIONE INVIATA DA DIRETTORI DI SOC OSPEDALIERE E/O RESPONSABILI SOS DIPARTIMENTALI OSPEDALIERE PER COMPETENZA AI SOLI DIRETTORI DI DIPARTIMENTO E PER CONOSCENZA A DIVERSE STRUTTURE AZIENDALI DOTATE DI PROTOCOLLO INFORMATICO *(comportano SEMPRE la protocollazione da parte del 1° servizio in indirizzo collegato sulla rete di protocollazione ARCHIFLOW.*

Sarà quindi il primo servizio aziendale presente tra i destinatari e in possesso dell'accesso alla rete di protocollazione ARCHIFLOW. a protocollare in arrivo la comunicazione dando la competenza al Dipartimento e tutte le conoscenze ai servizi aziendali in indirizzo.

3B) COMUNICAZIONE INVIATA DA DIRETTORI DI SOC OSPEDALIERE E RESPONSABILI SOS DIPARTIMENTALI PER COMPETENZA AI SOLI DIRETTORI DI DIPARTIMENTO E PER CONOSCENZA A DIVERSE STRUTTURE AZIENDALI DOTATE DI PROTOCOLLO INFORMATICO TRA CUI LA DIREZIONE GENERALE *(comportano SEMPRE l'inserimento per conoscenza della DSO)*

Il Protocollo Generale è tenuto alla protocollazione in arrivo della comunicazione in questione .

(con la competenza attribuita al Direttore di Dipartimento e la visibilità per conoscenza alle restanti strutture in indirizzo)

LA STESSA PROCEDURA DEL PUNTO 3A) DEVE AVVENIRE QUALORA UN DIRETTORE DEL DIPARTIMENTO SCRIVA AL SOLO DIRETTORE DI SOC OSPEDALIERA

LA STESSA PROCEDURA DEL PUNTO 3B) DEVE AVVENIRE QUALORA UN DIRETTORE DEL DIPARTIMENTO SCRIVA PER COMPETENZA AL SOLO DIRETTOR DI SOC OSPEDALIERA E SOS DIPARTIMENTALE E PER CONOSCENZA A DIVERSE STRUTTURE AZIENDALI

LA STESSA PROCEDURA DEL PUNTO 3B) DEVE AVVENIRE QUALORA UN DIRETTORE DEL DIPARTIMENTO SCRIVA PER COMPETENZA AL SOLO DIRETTOR DI SOC OSPEDALIERA E/O RESPONSABILE SOS DIPARTIMENTALE OSPEDALIERA E

PER CONOSCENZA A DIVERSE STRUTTURE AZIENDALI TRA CUI LA DIREZIONE GENERALE

4) COMUNICAZIONE DI UN DIRETTORE DI SOC OSPEDALIERA E/O RESPONSABILE SOS DIPARTIMENTALE OSPEDALIERA AD UN ALTRO DIRETTORE DI SOC OSPEDALIERA E/O RESPONSABILE SOS DIPARTIMENTALE OSPEDALIERA *dovrà essere inviata SEMPRE anche alla D.S.O. che addiverrà alla protocollazione in arrivo per competenza alla DSO stessa attribuendo le conoscenze ai servizi eventualmente individuati dal Primario mittente.*

Ricordarsi che se compare tra i destinatari la Direzione Generale sarà il PROTOCOLLO GENERALE a protocollare

5) COMUNICAZIONE DI UN DIRETTORE DI DIPARTIMENTO AD UN ALTRO DIRETTORE DI DIPARTIMENTO NON IN RETE SULLA PROCEDURA ARCHIFLOW *dovrà essere inviata SEMPRE per conoscenza alla DSO che addiverrà alla protocollazione in arrivo per competenza al Direttore del Dipartimento destinatario attribuendo le conoscenze ai servizi eventualmente individuati dal Direttore di Dipartimento mittente.*

Ricordarsi che se compare tra i destinatari la Direzione Generale sarà il PROTOCOLLO GENERALE a protocollare.

Protocolla la prima struttura presente tra i destinatari. Qualora compaia per conoscenza o competenza la Direzione Generale protocolla per tutti il PROTOCOLLO GENERALE

6) COMUNICAZIONE DI UN DIRETTORE DI DIPARTIMENTO O DI UN DIRETTORE DI SOC OSPEDALIERA E/O RESPONSABILE DI SOS DIPARTIMENTALE OSPEDALIERA AD UNA O PIU' STRUTTURE AZIENDALI PER COMPETENZA.

Rammentando che comunque la comunicazione va sempre inviata per conoscenza alla DSO, la prima struttura in indirizzo per competenza protocollerà in arrivo la comunicazione, attribuendo le altre competenze e le eventuali conoscenze così come indicate in indirizzo. QUALORA COMPAIA LA DIREZIONE GENERALE SARA' QUEST'ULTIMA A PROTOCOLLARE.

SI RIBADISCE CHE IN CASO DI POSTA IN PARTENZA DA STRUTTURE AZIENDALI A DIRETTORI DI SOC E SOS DIPARTIMENTALI OSPEDALIERE LA COMUNICAZIONE DOVRA' SEMPRE RIPORTARE TRA I DESTINATARI PER CONOSCENZA ANCHE LA DSO (CHE RICOMPRENDE ORA ANCHE LA STRUTTURA DI ASSISTENZA SPECIALISTICA AMBULATORIALE)

7) COMUNICAZIONI INVIATE DA PERSONALE DIPENDENTE AI PROPRI RESPONSABILI LE CUI STRUTTURE SONO DOTATE DI PROTOCOLLO INFORMATICO
(leggasi per esempio corrispondenza del personale SITRPO con i propri responsabili).
La struttura aziendale che riceve la comunicazione provvederà ad acquisirla tramite la protocollazione in arrivo (ovviamente qualora debba essere dato valore probatorio al contenuto della stessa).

2.B12 Invio dei documenti da struttura aziendale in rete sul protocollo informatico verso altre strutture aziendali interne

Il documento inviato ad una struttura interna viene protocollato in partenza dalla struttura che redige il documento stesso e la struttura ricevente non dovrà compiere nessun atto aggiuntivo di registrazione.

Parte Terza

Il protocollo di rilevanza giuridico-probatoria: la Registrazione

3. Registrazione e timbro di protocollo (segnatura)

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi vanno protocollati.
Il protocollo serve, infatti, ad attribuire ad un determinato documento data, forma e provenienza certa attraverso la registrazione dei seguenti elementi rilevanti sul piano giuridico–probatorio:
a) data di registrazione;
b) numero di protocollo;
c) mittente per il documento in arrivo; destinatario per il documento in partenza;
d) oggetto;
e) visibilità e notifica informatica
L'insieme di tali elementi è denominato «Registrazione».
Il sistema deve prevedere anche la registrazione, se ocumento in arrivo e se disponibili, dei seguenti elementi:
a) data, se presente, del documento ricevuto;
b) numero di protocollo, se presente, del documento ricevuto.

Nel caso dei documenti informatici, il sistema prevede anche la registrazione dell'impronta, cioè di una sequenza di caratteri che identificano in maniera univoca il documento.

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.
La registrazione e la segnatura costituiscono un'operazione unica e contestuale avente entrambe la natura di atto pubblico.
Nel documento in arrivo dall'esterno la segnatura viene posta sul frontespizio attraverso apposizione di un timbro meccanico, etichetta, barcode, etc. avente le seguenti caratteristiche:

ASL V.C.O.
Numero protocollo/anno
Data protocollo
Competenza (n° tabellari struttura)
Conoscenza (n° tabellari strutture)

Il timbro/ etichetta /copertina informatica (quest'ultima nel caso di Posta Elettronica Certificata e di e-mail ordinaria) si divide in quattro parti.
Nella prima parte è individuata l'area organizzativa omogenea *(A.S.L. V.C.O.)*; nella seconda parte vanno riportati gli elementi per la gestione del documento, cioè del *records management (Numero , anno)*; nella terza parte vanno segnati gli elementi identificativi della struttura/e individuata quale competente; nella quarta parte vanno segnati gli elementi identificativi della /delle strutture individuate per conoscenza.

Ad avvenuta approvazione del titolario di classificazione la struttura assegnataria per competenza dovrà addivenire all'inserimento della classificazione entro tre giorni dal ricevimento sulla piattaforma gestionale documentale archi flow.

3.1 Monitoraggio del workflow attraverso il timbro di protocollo

Gli elementi sopradescritti si completano nel prosieguo del workflow come segue:

a) il servizio protocollo provvede all'apposizione del numero e della data di registrazione, nonché alla individuazione della struttura di competenza e di altre strutture per conoscenza ;
b) il servizio protocollo provvede anche alla eventuale correzione dello smistamento ad una struttura, tenendo conto della storicizzazione delle assegnazioni, registrando cioè data e denominazione dei precedenti assegnatari di analogo
documento. **Con il presente Manuale si dispone che, qualora la competenza o la conoscenza assegnata ad una struttura risulti errata, quest'ultima sia tenuta a darne comunicazione entro tre giorni dalla segnatura al protocollo generale UNICAMENTE attraverso la casella mail dedicata** "gestionecorrispondenza@aslvco.it" **facendo pervenire l'originale cartaceo (se presente) con annotazione a mano a fianco della segnatura "NON COMPETENTE", data e firma leggibile**. Trascorsi i tre giorni dalla segnatura di protocollo non verrà più effettuata variazione se non su espressa richiesta della Direzione aziendale. Sarà quindi allora compito della struttura che ha ricevuto la comunicazione per competenza trasmetterla al servizio competente o ai servizi aggiuntivi che ritiene debbano ricevere per conoscenza la comunicazione con lettera protocollata inviandola per conoscenza via mail a gestionecorrispondenza@aslvo.it al fine di consentire successivamente di non ripetere l'errore di assegnazione. Si rammenta che per ottemperare alle vigenti disposizioni in tema di privacy è bene ridurre anche le assegnazioni per conoscenza affinchè sia il servizio competente a valutare correttamente quali altri attori aziendali debbano essere coinvolti nel procedimento.
Ad avvenuta variazione da parte del protocollo generale verrà inoltrata risposta via mail. Tale corrispondenza informatica verrà allegata al documento protocollato attraverso la procedura gestionale ARCHIFLOW ad attestazione della storia delle variazioni di assegnazione.
c) i Responsabili di struttura complessa, semplice dipartimentale, di Macrostruttura e/o di dipartimento strutturale provvedono ad assegnare il documento al Responsabile di struttura e/o al Responsabile del Procedimento Amministrativo (RPA).
d) Il RPA provvederà, ad avvenuta attivazione del titolario di classificazione e mediante gli operatori interni di protocollo, alla sua classificazione e fascicolazione, segnandovi anno e numero dell'unità archivistica (fascicolo o sottofascicolo).
Non è necessario il timbro sul documento in partenza; i dati della registratura e gli elementi necessari al workflow vanno apposti direttamente dal RPA, o dagli operatori del protocollo di struttura, sul documento secondo le consuetudini e l'impostazione grafica del modello istituzionale.
Alle singole registrazioni di protocollo solo legati i documenti informatici o le copie immagine acquisite con lo scanner. In quest'ultimo caso viene fatta salva la possibilità di escludere alcuni documenti per motivi di tutela della riservatezza. Deve però essere citata tale motivazione nelle annotazioni.

3.2 Registrazioni con differimento dei termini di accesso

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza temporanea delle informazioni, cioè il differimento dei termini di accesso (ad esempio, gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso al protocollo unico con annotazione.
Il responsabile dell'immissione dei dati deve indicare nelle annotazioni contestualmente alla registrazione di protocollo anche l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate divengono soggette al diritto di accesso nelle forme previste dalla normativa vigente.

3.3 Protocollo differito

Nel caso di un temporaneo ed eccezionale carico di lavoro che non permette di evadere la corrispondenza ricevuta entro il giorno successivo al ricevimento e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di

domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del responsabile del servizio di protocollo è autorizzato l'uso del protocollo differito. Il protocollo differito consiste nel differimento dei termini di registrazione, cioè nel provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve comunque essere effettuata.
Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il responsabile del servizio di protocollo deve descrivere nel provvedimento.
Resta preciso obbligo in capo ai Direttori di Struttura Aziendali o loro delegati segnalare al protocollo generale con mail indirizzata a gestionecorrispondenza@aslvco.it la data di scadenza di gare di particolare entità o di concorsi al fine di una corretta organizzazione del lavoro.

3.4 Il protocollo RISERVATO (particolare)
Sono previste particolari forme di riservatezza e di accesso collegate al protocollo unico per:
a) documenti legati a vicende di persone o a fatti privati o particolari;
b) documenti di carattere politico e di indirizzo di competenza del Direttore Generale o del Direttore amministrativo o Sanitario che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
c) documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
d) le tipologie di documenti individuati dalla normativa vigente (in particolare dall'art. 24 della legge 7 agosto 1990 n. 241 e s.m.i., dall'art. 8 del DPR 27 giugno 1992 n. 352 e dalla serie di norme collegate al D.Lgs. 196/2003 e s.m.i.);
I documenti registrati con tali forme appartengono al cosiddetto *Protocollo particolare*,cioè ad un repertorio del protocollo unico.
Le tipologie di documenti da registrare nel protocollo particolare sono individuati dal responsabile del protocollo informatico in collaborazione con l'organo monocratico (DIRETTORE GENERALE) e d'intesa con i responsabili delle strutture complesse.
Sono istituiti i seguenti PROTOCOLLI RISERVATI:
DIRETTORE GENERALE, SANITARIO ED AMMINISTRATIVO AZIENDALE (unico)
DIRETTORE DIPARTIMENTO PREVENZIONE (per i Servizi SIAN E SPRESAL)
SERVIZIO ISPETTIVO
UFFICIO PROCEDIMENTI DISCIPLINARI
L'utilizzo degli stessi è personale o attribuito a propri delegati mediante provvedimento espresso e mediante procedure particolari con accesso riservato, con livelli di accesso predeterminati.
Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la protocollazione, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti e procedimenti amministrativi, ad eccezione della scansione ottica (documento in arrivo) o dell'associazione del file (documento in partenza) che possono non essere effettuate. In caso di documento informatico lo stesso deve essere acquisito nella sua completezza.
Il complesso dei documenti registrati con il protocollo particolare costituisce una sezione particolare del protocollo unico.
A protezione dei dati personali, il documento cartaceo pervenuto per posta al PROTOCOLLO GENERALE (la cui tipologia rientra tra quelli del protocollo particolare) verrà trasmesso in busta chiusa direttamente al:
-DIRETTORE GENERALE per la conseguente protocollazione
- AL DIRETTORE DEL DIPARTIMENTO DI PREVENZIONE per la protocollazione e conseguente trasmissione ai Direttori SIAN E SPRESAL
- alla segreteria del SERVIZIO ISPETTIVO
- alla segreteria dell'UFFICIO PROCEDIMENTI DISCIPLINARI

Ciò ovviamente se sulla busta comparirà una modalità di identificazione della tipologia del documento riservato.

3.5 La protocollazione dei certificati di malattia su un repertorio del sistema documentale esterno al protocollo generale

La SOC Gestione delle Risorse Umane provvede giornalmente a scaricare dalla procedura dell'INPS i certificati di malattia riguardanti personale dipendente dell'ASL VCO. Ad ogni certificato elettronico viene assegnato informaticamente un numero di repertorio e gli operatori della SOC Gestione delle Risorse Umane provvedono all'assegnazione informatica per competenza dei certificati. I Direttori di SOC, SOS Dipartimentali assegnatari di personale sono tenuti ad aprire giornalmente la procedura e si troveranno nella casella di posta per competenza i certificati. Il sistema mantiene traccia di ogni visualizzazione.

3.6 Consegna dei documenti analogici ed informatici dal protocollo alle strutture aziendali

-Documenti Analogici - Esauriti gli adempimenti di cui ai precedenti punti, i documenti cartacei, protocollati dal Protocollo Generale e assegnati, e la posta che non necessita di protocollazione, sono resi disponibili ai destinatari individuati quali assegnatari per competenza presso l'Ufficio Protocollo nelle relative caselline di smistamento della corrispondenza ed inoltrate, tramite servizio di navetta interna od autista dedicato, alle strutture competenti site in altre sedi aziendali

- Documenti Informatici - Il sistema gestionale documentale in uso presso la nostra Azienda consente l'assegnazione informatica per competenza e conoscenza alle singole strutture. La casella di "posta" per competenza deve essere aperta giornalmente e ne rimane traccia sul sistema informatico gestionale. La responsabilità di ottemperare a tale obblighi e di vigilare è in capo al Direttore della struttura che può delegare per iscritto tale compito ad altro personale afferente.

3.7 Annullamento di una registrazione

È consentito l'annullamento di una registrazione di protocollo solo attraverso l'apposizione informatica della dicitura «annullato», che deve essere effettuata in maniera tale da consentire la lettura delle informazioni registrate in precedenza da parte del Responsabile del Protocollo e da non alterare le informazioni registrate negli elementi obbligatori del protocollo.

Solo il Responsabile del servizio di protocollo informatico e suo delegato da individuare con lettera scritta sono autorizzati ad annullare i documenti. Ad esso vanno trasmesse le richieste scritte, analogiche o informatiche sottoscritte digitalmente, di annullamento debitamente protocollate a firma del Direttore della Struttura interessata, contenenti il numero di protocollo da annullare, i motivi dell'annullamento.

Nel record di protocollo devono apparire in forma ben visibile, oltre agli elementi già indicati, anche data e ora dell'annullamento, nonché il codice identificativo o il nominativo dell'operatore che ha effettuato l'annullamento.

3.8 Documenti da non protocollare

gazzette ufficiali
bollettini ufficiali P.A.
notiziari P.A.
note di ricezione circolari
note di ricezione altre disposizioni
materiali statistici
atti preparatori interni
giornali riviste libri
materiali pubblicitari
inviti a manifestazioni che non attivino procedimenti amministrativi

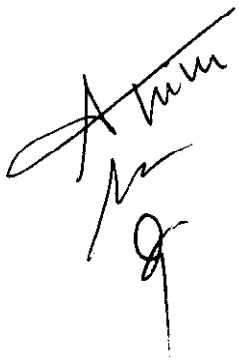
fatture (attive e passive)
certificati medici
visite fiscali (si protocollano solo quelle "sfavorevoli" al dipendente, ad es. quelle per cui è stata riscontrata un'assenza al controllo)
richiesta di rimborso spese e missioni di commissari (e non) interni ed esterni
tutti i documenti già soggetti a registrazione particolare dell'amministrazione

3.9 Lettere anonime e lettere prive di firma

Lettere anonime. La *ratio* che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntata alla avalutatività.
In altre parole, il protocollista deve attestare che un determinato documento così come si registra è pervenuto. Si tratta dunque di una delicata competenza di tipo notarile, attestante la certezza giuridica di data, forma e provenienza per ogni documento.
Le lettere anonime, pertanto, vanno protocollate.
In questi casi, la procedura prevede l'utilizzo del protocollo RISERVATO DEL DIRETTORE GENERALE, cioè di un repertorio all'interno del protocollo unico (quindi con l'unicità del numero di protocollo).
Le lettere prive di firma vanno protocollate.
A maggior ragione quando si tratta di un concorso (è il caso più critico). Se, come avviene in alcuni uffici di protocollo, si avvisa l'autore (o identificato come tale) della mancanza della firma e lo si invita a sanare la situazione presso l'ufficio protocollo, in realtà si danneggiano i terzi, a causa della eventuale mancata esclusione dal concorso del candidato che ha omesso la firma (qualora tale mancanza comporti la nullità dell'atto stesso). Agli addetti alla registratura spetta solo il compito di certificare che *quel* documento è pervenuto in *quel* modo e in *quelle* forme determinate.
La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. Sarà poi compito della struttura complessa, Dipartimento, e in particolare, del RPA valutare, caso per caso la sua efficacia riguardo ad un affare o un determinato procedimento amministrativo, cioè se la lettera priva di firma è ritenuta valida, nulla, sanabile.

3.10 Registro giornaliero e annuale di protocollo

Quotidianamente è garantito il *back-up* di tutti i dati del sistema di gestione documentale. Giornalmente viene generato il registro di protocollo. Il sistema esporta gli estremi di segnatura/registrazione su un file txt che viene convertito in formato PDF/A e firmato digitalmente e con marca temporale da parte del Responsabile della SOC AFFARI GENERALI o suo delegato. Gli operatori di protocollo creano successivamente una copia su supporto rimovibile non riscrivibile e lo consegnano al Direttore della SOC Informatione Comunication Tecnology per la conservazione.
Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.



Parte Quarta

Il protocollo ed il sistema documentale gestionale

4. Responsabilità della gestione del flussi documentali e degli archivi

I Dirigenti Responsabili delle singole strutture, sono garanti, in conformità alle disposizioni di cui al presente manuale, della gestione dei documenti analogici, dalla fase della loro formazione a quella della loro conservazione e dell'accesso agli archivi, anche nel caso in cui le modalità di gestione dovessero comportare l'esternalizzazione di determinati servizi.

Ogni azione amministrativa comporta la produzione, la tenuta e la conservazione di documentazione archivistica.

In un sistema di gestione e tenuta dei documenti ciò che conta non è il documento in quanto tale, ma l'insieme delle relazioni che quel documento ha con tutti gli altri (cioè l'intero archivio) e, più in particolare, con quelli che riguardano un medesimo affare o un medesimo procedimento amministrativo. Ecco alcuni esempi di casistica generale:

4.1 Documentazione di competenza di altre amministrazioni o di altri soggetti

Qualora pervenga all'Azienda un documento cartaceo di competenza di un'altra amministrazione o destinato ad altra persona fisica o giuridica, se lo stesso non è stato aperto viene riconsegnato al vettore postale per la corretta consegna. Se è stat erroneamente aperta la busta la comunicazione viene protocollata con assegnazione alla SOC AFFARI GENERALI che provvederà, con lettera protocollata di accompagnamento, alla ritrasmissione al destinatario. Il documento protocollato in arrivo non deve essere annullato ma nelle note dovrà comparire la frase " Non di competenza ASL VCO. Ritrasmesso con nota prot n...." Nel caso in cui il mezzo di trasmissione sia informatico il documento sarà protocollato con le stesse modalità sopra citate e con lettera protocollata ne verrà data informazione al mittente, con l'utilizzo dello stesso mezzo informatico, specificando che la documentazione trasmessa non risulta di competenza dell'ASL VCO.

4.2 Registrazione "a fronte"

Ogni documento è individuato da un unico numero di protocollo. Non è pertanto consentita la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza, neppure se l'affare si esaurisce con la risposta e neppure se la registrazione avviene nel medesimo giorno lavorativo.

4.3 fax

Il documento ricevuto a mezzo fax necessita di fotoriproduzione qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione.

Verificato che sia indicata la fonte di provenienza (deve cioè comparire il firmatario del documento), l'uso del fax soddisfa il requisito della forma scritta e, quindi, il documento può non essere seguito dalla trasmissione dell'originale.

L'accertamento della fonte di provenienza, (nel caso di dubbi specifici a riguardo) spetta al responsabile della struttura complessa e/o RPA che riceve per competenza il fax in questione ed avviene di norma per le vie brevi o con l'uso dei sistemi informatici.

Si rammenta che anche il documento in partenza può essere inviato via fax e, qualora non sia una semplice anticipazione del documento originale, dovrà recare la dicitura "**COMUNICAZIONE UNICA**". Il Responsabile del procedimento amministrativo è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta.

Si ponga attenzione a riportare la segnatura non tanto sulla copertina di trasmissione, quanto piuttosto sul documento medesimo. A questo proposito si sottolinea l'inutilità della copertina di trasmissione qualora il documento abbia una funzione prevalentemente informativa e non giuridico-probatoria.

Poiché ai sensi CAD tra le pubbliche amministrazioni corre l'obbligo di trasmettere corrispondenza mediante l'uso della posta elettronica certificata il protocollista provvederà alla segnatura di protocollo ma il R.P.A. dovrà, qualora la comunicazione provenga da una P.A. con esclusione dell'autorità giudiziaria, inoltrare una nota alla P.A. mittente al fine di chiedere che le comunicazioni a venire siano trasmesse a mezzo PEC. Ciò in quanto dall'11 agosto 2016 le P.A. incorreranno in sanzioni se non ottempereranno all'obbligo di completa dematerializzazione.

4.4 Fax seguito dall'originale

Ogni documento deve essere individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione. Di conseguenza qualora venga registrato un documento ricevuto via fax e venga successivamente ricevuto lo stesso documento in originale, gli operatori del PROTOCOLLO GENERALE e/o gli operatori di protocollo presenti nelle strutture aziendali autorizzati alla protocollazione in arrivo ai sensi dell'allegato 1 al presente provvedimento devono attribuire all'originale la stessa segnatura del documento pervenuto via fax. Si tratta infatti del medesimo documento pervenuto precedentemente via fax, su diverso supporto e con un diverso mezzo di trasmissione.

Il timbro di protocollo (segnatura) va posto sul documento e non sulla copertina di trasmissione del fax.

Gli OPERATORI DEL PROTOCOLLO GENERALE e/o gli operatori del protocollo delle strutture aziendali devono comunque accertare che si tratti del medesimo documento; qualora vi fosse qualche correzione, anche minima, si tratterebbe di un documento *diverso* e quindi andrà registrato con un nuovo numero di protocollo.

Il tipico esempio è rappresentato da un documento in arrivo via fax senza firma, data e protocollo ma con l'indicazione nominativa del firmatario. L'originale pervenuto successivamente con firma va protocollato con un nuovo numero.

4.5 Modello organizzativo per individuare i documenti già registrati (fax, originali plurimi, etc.)

Il responsabile del servizio di protocollo informatico deve organizzare la procedura informatica per individuare, di norma, il documento originale pervenuto "qualche giorno prima" via fax, ipotizzando il fatto che l'addetto alla registratura non sia lo stesso per il fax e per l'originale. La procedura si riferisce anche ai documenti ricevuti in originali plurimi in quanto indirizzati a più uffici od organi, i quali pervengono al protocollo in giorni diversi.

Nel caso di posta in arrivo inviata dall'esterno è opportuno che le ditte, le AS.SS.LL., e tutti i soggetti esterni siano, qualora possibile, invitati dai Responsabili di struttura a scrivere sull'originale della lettera che perverrà successivamente " GIA'ANTICIPATA VIA FAX".

Nel caso di posta in arrivo inviata via fax dall'esterno, senza successivo inoltro di originale, sarà opportuno che sia indicato COMUNICAZIONE UNICA.

Verificata la registrazione dello stesso documento, gli operatori del protocollo generale e/o dei protocollo delle strutture provvedono alla apposizione degli stessi elementi della segnatura del documento già registrato.

Pur essendo stata superata la fase iniziale di applicazione del manuale di gestione qualora eccezionalmente si riscontri che lo stesso documento (anticipato via Fax e successivamente inviato in originale) abbia acquisito due numeri di protocollo si richiamerà il documento inserito per

ultimo e si inserirà nelle "annotazioni" DOCUMENTO GIA' PROTOCOLLATO IN DATA..... CON NUMERO.....

4.6 Posta elettronica (e-mail ordinaria)

I messaggi di posta elettronica che soddisfano i requisiti indicati dalla normativa vigente vanno protocollati .

L'eventuale segnatura di protocollo dovrà rispettare lo standard XML.

A tal fine, L'A.S.L. V.C.O., ha attivato una casella di posta elettronica adibita a finalità di protocollazione, con comunicazione alla CNIPA per l'inserimento nell'indice delle Amministrazioni Pubbliche.

Preso altresì atto che le e-mail inoltrate da privati e da soggetti esterni all'azienda (non enti pubblici) risultano una importante modalità di comunicazione, nel rispetto delle vigenti disposizioni si stabilisce che la protocollazione in arrivo delle stesse possa addivenire per tutte le tipologie di documenti fatti i salvi in cui la normativa dispone diversamente. L'accertamento della fonte di provenienza, (nel caso di dubbi specifici a riguardo) spetta al responsabile della struttura complessa e/o RPA che riceve per competenza la e-mail in questione ed avviene di norma per le vie brevi o con l'uso dei sistemi informatici.

E' vietato l'utilizzo delle caselle istituzionali, sia di struttura che personali, per comunicazioni non attinenti all'attività dell'Azienda.

Nel formato dei messaggi di posta elettronica ordinaria è inserito automaticamente il seguente testo: *"Ai sensi del D.lgs. n. 196 del 30.06.03 (Codice Privacy), le informazioni contenute nella presente comunicazione sono riservate e ad uso esclusivo del destinatario. La diffusione e/o fotocopiatura del presente documento e di eventuali allegati da parte di qualsiasi soggetto diverso dai destinatari è proibita; tale divieto di diffusione è sanzionato sia dall'art. 616 c.p. (violazione, sottrazione e soppressione di corrispondenza) che dal D.L.gs. 196/03. Qualora il messaggio fosse pervenuto per errore, La preghiamo di eliminarlo senza copiarlo ovvero inoltrarlo a terzi, dandocene gentilmente immediata comunicazione".*

4.7 La posta elettronica ordinaria nelle comunicazioni interne all'Azienda

Le comunicazioni tra l'Azienda e i dipendenti, nonché tra le varie articolazioni aziendali, avvengono, di norma, mediante l'utilizzo della casella di posta elettronica ordinaria dei rispettivi dipartimenti/servizi/uffici o le caselle di posta elettronica individuali, nel rispetto delle norme in materia di protezione dei dati personali.

La posta elettronica viene utilizzata per:

- convocare riunioni (interne all'Azienda, o esterne purché a basso livello di formalità);
- inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito a informazioni generali di organizzazione;
- diffondere circolari e ordini di servizio;
- diffondere rappresentazioni digitali di documenti cartacei regolarmente protocollati. In tal caso, i documenti acclusi al messaggio sono trasmessi in copia immagine o in formato ".pdf".
- inoltrare ai direttori di struttura o sos dipartimentali la relazione finale di chiusura di un reclamo

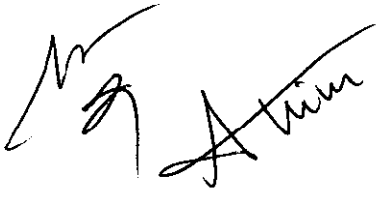
4.8 Posta elettronica certificata

L'e-mail è certamente uno dei mezzi di comunicazione più diffuso per la sua economicità e l'immediatezza di trasmissione. Presenta però dei punti deboli, quali, ad esempio, la possibilità di falsificare il mittente o l'orario di invio, che hanno indotto a ricercare forme di comunicazione più sicura, come appunto la **Posta Elettronica Certificata (PEC), nata per assicurare agli utenti la certezza, il valore legale, l'invio e la consegna (o meno) dei messaggi e-mail al destinatario.** Per molti aspetti simile al modello cartaceo della raccomandata con ricevuta di ritorno, si differenzia da quest'ultima in quanto *la PEC permette di conoscere con certezza il mittente reale del messaggio, assicurando così la possibilità di legare in maniera certa ed inopponibile la*

trasmissione con il documento trasmesso. Inoltre, rispetto alla raccomandata A/R, la PEC presenta ulteriori vantaggi: semplicità ed economicità di archiviazione, inoltro e riproduzione; facilità di invio a più destinatari contemporaneamente con costi decisamente irrisori; possibilità di consultazione ed uso anche da postazione diverse da quelle del proprio ufficio o abitazione ed in qualunque momento, grazie alla persistenza del messaggio nella casella di posta elettronica. I soggetti coinvolti nella trasmissione di documenti informatici tramite il sistema della PEC, sono il mittente del messaggio, il gestore del mittente, cioè il soggetto con il quale il mittente ha un rapporto per poter usufruire del servizio di PEC, il gestore del destinatario, cioè il soggetto con il quale il destinatario mantiene un rapporto per usufruire del servizio di PEC, il destinatario del messaggio. Prima di procedere all'analisi pratica della trasmissione di documenti informatici tramite PEC, è bene anticipare qualche informazione sui cosiddetti Gestori ovvero le aziende, anche Pubbliche Amministrazioni, che possono offrire il servizio di Posta Elettronica Certificata, dopo aver dimostrato di essere in possesso dei requisiti richiesti dalla normativa di riferimento e dopo essere stati iscritti in un apposito elenco pubblico tenuto dal CNIPA. In particolare, i Gestori si occupano di garantire le fasi di invio e di consegna di un messaggio, oltre che ovviamente rilasciare caselle e domini PEC.

Il processo di trasmissione del documento informatico attraverso la PEC, inizia con il riconoscimento del mittente da parte del proprio gestore di PEC attraverso modalità determinate che possono essere la tradizionale accoppiata user-id/password oppure modalità che si basano su supporti quali, ad esempio, la smart-card. Dopo la fase di riconoscimento, il mittente invia il messaggio di PEC, utilizzando l'interfaccia disponibile che può essere un web browser oppure un client di posta elettronica. Il mittente, attraverso la PEC, ha la possibilità di inviare qualsiasi tipo di documento informatico, ad es. un testo, un'immagine, un applicazione e così via. Una volta che il mittente ha inviato il messaggio, quest'ultimo viene sottoposto ad una serie di controlli da parte del gestore della PEC del mittente, controlli che sono finalizzati alla verifica della correttezza formale del messaggio e dell'assenza di virus. Nel caso in cui i controlli abbiano esito negativo, il messaggio non viene inviato al destinatario ed il mittente riceve una ricevuta, firmata elettronicamente dal proprio gestore, nella quale si dà avviso del mancato recapito del messaggio e le relative motivazioni. Nel caso in cui, invece, i controlli abbiano esito positivo, il gestore del mittente firma elettronicamente il messaggio da inviare, al fine di garantirne l'inalterabilità, e lo inoltra al gestore del destinatario. Quest'ultimo, ricevuto il messaggio, provvede ad una serie di controlli per verificare la provenienza del messaggio (da un gestore PEC iscritto nell'apposito elenco) e l'integrità del messaggio ricevuto, sempre al fine di garantirne la non alterazione nel transito da un gestore all'altro. Anche in questo caso, se i controlli effettuati hanno esito negativo, il gestore del destinatario blocca l'inoltro del messaggio al destinatario e notifica al mittente la mancata consegna e le relative motivazioni. In caso contrario, invece, il gestore del destinatario inoltra il messaggio nella casella di posta elettronica del destinatario e, in seguito, invia al mittente una ricevuta, firmata elettronicamente, di avvenuta consegna, che riporta anche il contenuto del messaggio inviato. Nel momento in cui il messaggio inviato diviene disponibile nella casella del destinatario si conclude il sistema di trasmissione della PEC, pertanto la lettura del messaggio da parte del destinatario è da considerarsi un'azione estranea ed esterna al processo di trasmissione. Inoltre, è utile specificare che, nell'ipotesi in cui il gestore verifichi la presenza di virus del messaggio, inviato o ricevuto, non solo non lo deve trasmettere, ma è obbligato a conservare il messaggio in un apposito archivio, il cosiddetto Log File, per una durata di trenta mesi, così come prescritto dalle norme, al fine di poter effettuare successive verifiche circa l'evento rilevato.

Occorre porre massima attenzione alla data di ricezione della PEC ai server certificatori di posta poiché, soprattutto qualora si debba determinare la data di avvio di un procedimento o un termine perentorio di presentazione di documentazione ecc., ***fa fede la data di ricezione al server di gestione della PEC dell'ASL VCO (INFOCERT-LEGALMAIL) che può anche non coincidere con la data di protocollazione.***



Tutte le PEC pervenute al protocollo dell'ASL VCO entro le ore 15,30 vengono infatti di norma protocollate in giornata ma le PEC che arrivano successivamente (anche durante la notte o il sabato e la domenica) vengono protocollate il giorno lavorativo successivo. Ecco che si viene a determinare una discrepanza tra la data di ricezione al server di gestione della PEC dell'ASL - *che contestualmente invia al mittente una ricevuta di avvenuta consegna* - e la data di protocollazione che risulta successiva.
Per determinare con esattezza la data di ricezione di una PEC è necessario leggere la PEC aprendo il messaggio dal sistema informatico ARCHIFLOW. Sul lato destro del messaggio è evidenziata data e ora di ricezione.
Nel caso di concorsi nel bando dovrà essere precisato che farà fede la data ed ora di avvenuta consegna all'ASL VCO della domanda attraverso PEC (e non solo l'avvenuto inoltro)

4.9 Comunicazioni dell'Azienda verso i privati (persone fisiche e giuridiche) ad avvenuta completamento dell'assegnazione della firma digitale.
Le comunicazioni formali e la trasmissione via posta elettronica di documenti, il cui contenuto impegna l'Azienda verso terzi, dovranno essere effettuate con posta elettronica istituzionale o posta elettronica certificata istituzionale per garantire la dematerializzazione che risulterà obbligatoria dal 11 agosto 2016.
Il documento inviato:
- se originariamente informatico, dovrà essere sottoscritto con firma elettronica avanzata, qualificata o digitale, ai sensi dell'art. 21 comma 2 del CAD;
- se originariamente analogico (cartaceo), dall'11 agosto 2016 dovrà esserne trasmessa una copia per immagine su supporto informatico; l'eventuale attestazione di conformità all'originale, ove richiesta, dovrà essere effettuata con le modalità di cui all'art. 23 *ter* comma 3 del CAD.

Qualora sia espressamente richiesto tale mezzo da parte del soggetto privato, le comunicazioni potranno avvenire via fax.
Potrà essere utilizzato il fax anche per rispondere ad un'istanza inviata con tale mezzo.
Ai sensi dell'art. 3-bis del CAD, il cittadino ha la facoltà di comunicare il proprio indirizzo di PEC rilasciato ai sensi dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, valido quale proprio domicilio digitale.
Qualora il cittadino abbia provveduto a comunicare il proprio domicilio digitale, secondo le modalità stabilite al comma 3 del suddetto articolo, ogni comunicazione che lo riguardi dovrà essergli notificata esclusivamente al domicilio dichiarato ed ogni altra forma di comunicazione non può produrre effetti pregiudizievoli nei suoi confronti.
A norma del successivo comma 4-bis dell'articolo citato, in assenza del suddetto domicilio digitale, è possibile predisporre – ad eccezione dei documenti che rappresentino delle certificazioni da utilizzarsi nei rapporti tra privati - le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare secondo le vigenti disposizioni, ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39 (Firmato nome e cognome e relativa qualifica) o prodotta attraverso il sistema di gestione documentale, avvalendosi del glifo o contrassegno elettronico.
In conformità all'art. 4-ter la copia analogica inviata al cittadino dovrà contenere una dicitura che specifichi che il documento informatico da cui la copia è tratta è stato predisposto e conservato presso l'Azienda in conformità alle vigenti regole tecniche.

4.10 Comunicazioni tra l'Azienda ed altre Pubbliche Amministrazioni

Le comunicazioni trasmesse dall'Azienda ad altre pubbliche amministrazioni sono effettuate mediante l'utilizzo della posta elettronica o della posta elettronica certificata, oppure attraverso sistemi di cooperazione applicativa. Il documento trasmesso deve essere firmato digitalmente non appena tutti i responsabili saranno dotati di firma digitale o, **se originariamente analogico/cartaceo, deve essere trasmesso in copia immagine.**

Le comunicazioni e i documenti informatici ricevuti da altre Pubbliche amministrazioni sono, ai sensi dell'art. 47 comma 2 del CAD, validi ai fini del procedimento una volta che ne sia verificata la provenienza ovvero quando:

- sono sottoscritti con firma elettronica qualificata o digitale;
- sono dotati di segnatura di protocollo;
- è comunque possibile accertarne la fonte di provenienza (es. apposizione di firma elettronica avanzata);
- sono trasmessi attraverso sistemi di posta elettronica certificata;

Ai fini della validità dell'avvio del procedimento amministrativo, ai sensi del D.P.C.M. 22 luglio 2011 e del Decreto Legge n. 18 ottobre 2012, n. 179, convertito con Legge 17 dicembre 2012 n. 221, è in ogni caso esclusa la trasmissione dei documenti a mezzo fax provenienti da Pubbliche amministrazioni.

4.11 Regole per la ricezione e la gestione dei messaggi di Posta Elettronica Certificata

La casella PEC istituzionale dell'Azienda è abilitata a ricevere sia messaggi provenienti da altre caselle PEC che messaggi provenienti da caselle di posta mail ordinaria. Gli operatori di protocollo provvederanno prioritariamente alla segnatura delle PEC e successivamente alla segnatura delle mail ordinarie.

Al fine di garantire una corretta gestione della documentazione pervenuta via PEC, anche sotto il profilo della conservazione, tutti i documenti pervenuti tramite tale sistema sono protocollati all'interno del sistema di gestione documentale fatta eccezione ovviamente per le comunicazioni non soggette a protocollazione già citate nel presente manuale.

Sono accettate le comunicazioni PEC provenienti da:

- caselle PEC di cittadini o imprese rilasciate ai sensi del D.P.C.M. 6 maggio 2009 e ss.mm. e ii., che stabilisce che a ciascun cittadino che ne faccia richiesta, il "Dipartimento per la digitalizzazione della Pubblica Amministrazione e per l'innovazione tecnologica assegni a titolo non oneroso un indirizzo di Posta Elettronica Certificata, da utilizzare per tutte le comunicazioni con la Pubblica Amministrazione"
- caselle PEC di cittadini o imprese rilasciate da gestori accreditati presso l'Agenzia per l'Italia Digitale (http://www.digitpa.gov.it/pec_elenco_gestori)
- caselle PEC di Pubbliche Amministrazioni e recanti gli estremi della segnatura di protocollo
- caselle PEC di Pubbliche Amministrazioni dotate di sistemi di interoperabilità conformi alle regole di cui alla circolare n. 60 del 23 gennaio 2013 di Agenzia per l'Italia Digitale

I documenti allegati devono avere le seguenti caratteristiche: formato aperto, stabile, completo, leggibile, non modificabile, privo di codici eseguibili, macro istruzioni, link. Si privilegeranno i formati già approvati da organismi di standardizzazione internazionali (ISO *International Organization for Standardization* e ETSI *European Telecommunications Standards Institute*).

I *file* trasmessi all'Azienda devono pervenire nei formati standard previsti dalla normativa vigente e coerenti con le regole tecniche del documento informatico e del sistema di gestione documentale.

Tra i formati ammessi si segnalano: PDF-PDF/A (estensione .pdf), TIFF (estensione .tif), JPG (estensione . jpg/.jpeg); testo (estensione .txt); *Office Open* XML - OOXML (estensione .docx, .xlsx, .pptx - standard ISO/IEC DIS 29500); *Open Document Format* - ODF (estensione .ods, .odp,

.odg, .odb - standard ISO/IEC DIS 26300); XML (estensione .xml); infine, in caso di *file* firmati digitalmente, i formati .p7m e .m7m.
Nell'ipotesi di invio di *file* compressi, i *file* originari dovranno essere nei formati suddetti.
La somma dei singoli *file* e della busta di trasporto non dovrà superare i 25 MB.
A ciascun messaggio trasmesso alla casella PEC dell'ASL VCO dovrà essere associato uno e un solo documento con gli eventuali allegati richiesti dal procedimento (es.: un fornitore che debba inviare n. 5 fatture, dovrà inviare n. 5 messaggi PEC distinti, uno per ciascuna fattura; un candidato che intenda partecipare a n. 2 diversi concorsi dovrà inviare n. 2 distinti messaggi PEC, uno per ogni domanda, corredata dagli allegati richiesti).

Se i *file* sono firmati digitalmente la firma digitale dovrà sottostare alle seguenti condizioni:
- firma riferita a *file* nei formati PDF/A, XML
- firma *embedded* ("incorporata" nel documento elettronico) e non *detached*
- firma valida al momento della ricezione da parte dell'ASL VCO
- *file* in formato .p7m oppure .m7m

Qualora i messaggi di posta elettronica contengano documenti prodotti con formati non conformi agli standard indicati dalla normativa vigente, il Responsabile del Procedimento provvederà, ove possibile, a regolarizzare la pratica richiedendo al mittente la trasmissione dei documenti nei formati richiesti, fermo restando che, nell'ipotesi di ricezione di *file* difformi, l'Azienda non può garantirne la leggibilità futura e la corretta conservazione.
I suddetti requisiti di accettabilità dei messaggi indirizzati alla casella PEC istituzionale sono anche pubblicati nell'apposita sezione "Posta Elettronica Certificata" del sito Internet aziendale.
Per la ricezione di determinate tipologie di documenti informatici (es. domande relative a bandi di gara, bandi di concorso, avvisi pubblici, ecc...) l'Azienda, nel rispetto della normativa vigente, può stabilire ulteriori e specifiche modalità di ricezione delle istanze da parte degli interessati, dandone previa comunicazione nei bandi e negli avvisi ad evidenza pubblica.

4.12 Firma Digitale

La firma digitale è il risultato di una procedura informatica – detta validazione – che garantisce l'autenticità e l'integrità di documenti informatici.
La firma digitale possiede le seguenti caratteristiche:

- **autenticità**: la firma digitale garantisce l'identità del sottoscrittore
- **integrità**: la firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione
- **non ripudio**: la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore

Come funziona
Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare.
La chiave privata è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento. Viceversa, la chiave da rendere pubblica è usata per verificare l'autenticità della firma.
Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza visto che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata.

4.13 Modelli pubblicati

L'Azienda si impegna a rendere disponibili sul sito Internet e/o sulla rete Intranet dell'Azienda l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad

ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.

4.14 Trasmissioni telematiche

Alcuni flussi di rendicontazione periodica sono trasmessi/ricevuti dall'Azienda con immissione diretta dei dati sul *server* dell'Ente destinatario, senza la produzione e conservazione dell'originale cartaceo.

Anche laddove non vengano trasmessi con firma digitale e sistema di crittografia, tali documenti sono comunque sempre inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca, attivate con i singoli Enti destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione. La conservazione di tale documentazione digitale é di competenza degli Enti destinatari.

4.15 Documentazione contabile

La documentazione contabile prodotta e ricevuta dall'Azienda non è protocollata, ed è registrata in apposito applicativo dedicato

4.16 Spedizione dei documenti informatici

La spedizione dei documenti informatici avviene con le procedure adottate dal Manuale operativo dello stesso ed una volte effettuate le operazioni di classificazione, fascicolazione (qualora attive) e protocollazione, e comunque secondo i seguenti criteri generali:

1) i documenti informatici sono trasmessi agli indirizzi elettronici dichiarati dai destinatari ovvero reperibili in indici ed elenchi ufficiali di pubblica consultazione (IndicePA per le pubbliche amministrazioni, INIPEC per imprese e professionisti, Ordini e collegi per i relativi iscritti ecc.) abilitati alla ricezione della posta per via telematica;

2) per la spedizione, l'Azienda si avvale delle caselle di posta elettronica istituzionali, della casella di posta elettronica certificata istituzionale

3) gli uffici utente abilitati alla protocollazione e gestione della PEC provvedono ad effettuare l'invio tramite P.E.C. mediante l'apposita funzione del sistema di gestione documentale, verificando l'avvenuto recapito dei documenti spediti per via telematica; le ricevute elettroniche sono archiviate in automatico dall'applicativo mediante associazione alle registrazioni di protocollo.

Per la riservatezza delle informazioni contenute nei documenti elettronici, gli addetti alla spedizione si attengono a quanto prescritto dall'art. 49 del CAD.

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni, senza che a queste l'Azienda riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

Parte QUINTA
5 Il sistema informatico

5.1 Tecnologie Standard

Per lo sviluppo della procedura informatica sono state utilizzate le tecnologie più diffuse ed affermate nel mercato dell'Information Technology, con l'obiettivo di permettere un efficace utilizzo dei sistemi operativi di ultima generazione.

5.2 Architettura CLIENT/SERVER

Per garantire la massima sicurezza ed integrità delle informazioni, vengono gestiti in modalità completamente client/server, sia l'accesso alla banca dati degli indici, sia la memorizzazione e la visualizzazione dei documenti. La soluzione WEB oriented è stata sviluppata utilizzando l'approccio a tre livelli (three-tier)

5.3 Gestione Organigramma Aziendale

Il sistema permette di rappresentare in maniera molto flessibile l'organigramma aziendale. L'Amministratore può definire utenti o gruppi di utenti ed uffici, anche in relazione gerarchica tra di loro. Ad ogni profilo di utenti o gruppo di utenti è possibile attribuire un insieme di diritti specifici, intesi come possibilità di eseguire azioni nel sistema (inserire, spedire, modificare ecc).

5.4 Gestione dei livelli di riservatezza

L'autenticazione all'accesso, le regole di accesso ai dati, ai flussi definiti o generati, garantiscono una capillare gestione della riservatezza. Oltre alla visibilità sul singolo archivio ed applicazione in lettura o scrittura, è possibile attribuire l'accesso anche sul singolo documento ad utenti, uffici e gruppi.

5.5 Soluzione distribuita in Wan ed in ambiente internet/intranet gestione dei Livelli di Assistenza

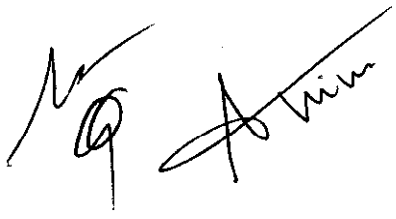
L'architettura e le tecnologie della procedura informatica in uso sono state progettate per garantire l'utilizzo sia in una rete locale, sia anche in rete geografica non performante. La versione WEB based è ovviamente utilizzabile in ambiente intranet/internet.

5.6 Applicazioni del Sistema

Il sistema in uso è in grado di archiviare e gestire qualsiasi tipo di file digitale e di supportare qualsiasi flusso documentale aziendale. L'Amministratore può realizzare senza la necessità di compilare scripting, applicazioni per la gestione del Protocollo Informatico, dei disegni tecnici, del ciclo attivo (spool di stampa) e passivo. Di ogni applicazione possono essere definiti il numero ed il tipo degli attributi e i diritti di accesso da parte dei membri dell'organigramma aziendale.

5.7 Fascicolazione

I Fascicoli del sistema, contenitori virtuali di documenti logicamente correlati, sono gestiti dal sistema come ultimo elemento di una struttura logica di archiviazione a tre o più livelli. Possono essere dotati di propri indici di classificazione, di una propria riservatezza e possono essere spediti internamente o via e-mail all'esterno.



5.8 Funzioni iniziali di workflow

Il Sistema in uso è dotato di un completo sistema groupware o work-flow cooperativo e di una serie di funzionalità per lo scambio di documenti e fascicoli tra i vari ruoli. La gestione dell'organigramma aziendale e l'integrazione con i più diffusi sistemi di posta elettronica permettono di costruire i flussi ed automatismi per il supporto documentale ai vari processi aziendali.

5.9 Produzione e conservazione delle registrazioni di protocollo informatico

Ogni registrazione di protocollo informatico produce un apposito record sul sistema centrale che viene accodato in una base dati accessibile esclusivamente al relativo motore. Anche gli stessi file contenenti la base dati non sono condivisi ma accessibili unicamente agli amministratori del sistema centrale. I campi non modificabili (numero e data di registrazione, mittente e destinatari, oggetto, numero e tipo di allegati) non sono alterabili da alcuno, nemmeno dall'amministratore. Le variazioni dei campi modificabili vanno riportate nel campo di annotazione.

Ogni operazione di inserimento e modifica viene registrata inoltre su un file di traccia prodotto dal motore in formato interno corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione. Da esso l'amministratore del sistema è in grado di ottenere l'elenco delle modifiche effettuate su una data registrazione ottenendo in dettaglio:

- nome dell'utente
- data e ora
- indirizzo della postazione di lavoro
- tipo di comando (inserimento/modifica/visualizzazione/cancellazione)

permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per copia conoscenza, restituzione, fascicolazione ecc.).

L'applicativo non consente di effettuare cancellazioni; in alternativa è previsto, per gli utenti abilitati, l'annullamento di un documento accompagnato da una motivazione. Dal punto di vista tecnico l'annullamento è una modifica di uno stato della registrazione ed è reversibile previa espressa motivazione di cui resta registrazione.

5.10 Sicurezza dei dati

La procedura informatica in uso è un'applicazione Client/server standard e tutte le comunicazioni tra il client ed il server e viceversa avvengono tramite una porta TCP. Queste possono essere cifrate così da renderle del tutto irriconoscibili ed inutilizzabili da "occhi Indiscreti".

Tutti i dati vengono gestiti dal motore server del database. L'accesso a questo avviene tramite nome utente + parola chiave ed è, in pratica, conosciuto solo dall'applicazione principale. Ne consegue che è possibile accedere ai dati di sistema, memorizzati nel database, solo da ARCHIFLOW. L'accesso all'applicazione avviene tramite nome utente + parola chiave anche queste cifrate con algoritmi diversi. Una proprietà del sistema permette il controllo nell'univocità di collegamento di un utente: in pratica può essere impedito o meno allo stesso di collegarsi da più postazioni contemporaneamente.

Ad ogni utente sono associati diversi diritti (direttamente e/o ereditati dai gruppi/uffici a cui appartiene nell'organigramma e/o tipi di documenti utilizzati) e sono questi che permettono all'utente di eseguire alcune operazioni ed altre no e di poter visualizzare/eseguire alcuni comandi al posto di altri.

Anche i documenti, così come avviene ai dati, vengono trasmessi dal client al server e viceversa attraverso una comunicazione, che può essere cifrata, su porta TCP.

Tutti i documenti, sia i principali che gli allegati, vengono memorizzati nel loto formato originale direttamente nel file system del server. L'accesso a quest'area è consentito al solo motore server del database. Quando l'applicazione richiede di visualizzarne uno, viene eseguita una copia dello stesso sul client, in questo modo si garantisce l'integrità dell'originale.

E' possibile sia inserire dei documenti già firmati da terzi, verificando la veridicità e la correttezza della firma, sia firmare dei documenti, precedentemente inseriti nel sistema. In questo secondo caso, naturalmente, è il lettore di smartcard, la smartcard e i driver CSP per la comunicazione con questa; i file firmati vengono incapsulati in una busta PKCS#7, il loro formato diventa così di tipo "firmato" (per la corretta visualizzazione è quindi necessaria prima la decodifica degli stessi, operazione che l'applicazione esegue in modo trasparente) e quindi viene creata l'impronta e memorizzata in modo non modificabile.

5.11 Registrazione dati di protocollo

Tutti i dati non modificabili (numero protocollo annuo a 7 cifre, data di registrazione, mittente/destinatari ed oggetto) vengono registrati nel database al momento dell'inserimento e non possono essere in nessun modo modificati successivamente.
E' possibile eventualmente modificare i campi che non hanno la proprietà di " non modificabilità" (proprietà personalizzabile per tipo di documento dall'amministratore di sistema) oppure possono essere aggiunte delle annotazioni o altri dati aggiuntivi; in ogni caso questa operazione come tutte le altre che si eseguono sulla scheda (inserimento dati, documenti, annotazioni , ecc.) vengono registrate, in modo non modificabile, in un'apposita sezione, la storia della scheda, che riporta oltre all'operazione la data con ora e l'autore. Inoltre è possibile eventualmente annullare una scheda da parte degli utenti che ne hanno diritto, specificando i motivi di tale operazione (anche questa soggetta a registrazione nella storia).
Un particolare modulo del sistema permette di tenere traccia (su file o carta) di tutti i numeri di protocollo man mano che questi vengono inseriti; questo permetterà di continuare a protocollare manualmente, a partire dall'ultimo inserito, nel caso di blocco del sistema (Registro di Emergenza).

5.12 Abilitazioni di accesso interno ed esterno

Livelli generali di accesso interno

Ci sono 3 possibilità:
a) Visibilità DOCUMENTI come indicato dal responsabile di struttura (totale o parziale)
b) Inserimento / modifica documento/ protocollazione
c) Annullamento
Per "Visibilità" si intende la possibilità per un utente abilitato di visualizzare una registrazione di protocollo, con l'esclusione dei documenti riservati;
Per "Inserimento/ modifica/protocollazione" si intende la possibilità per un utente abilitato di inserire i dati, provvedere ad una registrazione di protocollo, addivenire a successive modifiche nei campi modificabili, aggiungere eventuali annotazioni e la classificazione.
Con "Annullamento" si intende la possibilità per un utente abilitato (specificatamente il solo responsabile del protocollo informatico) di annullare una registrazione di protocollo.
Il Responsabile del servizio deve comunicare al RESPONSABILE DEL SISTEMA DI PROTOCOLLO richiesta scritta di abilitazione per ciascun utente.

5.13 AMMMINISTRATORE del protocollo informatico

È la persona, diversa dal responsabile del sistema informatico, che ha la possibilità di effettuare operazioni straordinarie sul sistema; ad es., il ripristino del sistema a seguito di eventuali interruzioni, il monitoraggio delle operazioni compiute, la predisposizione delle autorizzazioni di accesso al sistema, ecc.. (nella realtà aziendale dell'A.S.L. V.C.O. la individuazione dell'Amministrazione di sistema avviene con atto del Direttore della S.C. INFORMATION COMUNICATION TECNOLOGY).

5.14 Protocollista

Il protocollista (records manager) è la persona che è tenuta ad **aprire tutta la posta che giunge al protocollo** (anche quella nominativa in quanto se perviene al protocollo ASL VCO si ritiene essere correlata all'attività lavorativa con le eccezioni previste dal presente manuale) o a protocollare la posta in partenza. Le sole esclusioni di apertura delle buste riguardano casi specifici correlati ad atti giudiziari provenienti dal Tribunale e nominativi ed alle Gare oppure se compare la dicitura RISERVATO o PERSONALE o CONFIDENZIALE) ed è autorizzato ad eseguire la registrazione dei documenti, sia in arrivo, sia in partenza, sia scambiati tra uffici .

Egli può acquisire (a seconda dei diritti e del profilo con cui è registrata la sua utenza nel sistema) l'immagine elettronica del documento mediante uno scanner oppure associare il file prodotto da un programma di composizione testi o di elaborazione di fogli elettronici, o disegno a da mail, lotus. PEC. L'immagine elettronica od il file di testo possono essere registrati nel sistema nel momento della registrazione del documento.

Ad avvenuta adozione del titolario di classificazione nel caso dei documenti in partenza, il protocollista attribuirà al documento anche la prevista classificazione (titolo e classe) spedendo il documento ai destinatari .

5.15 Responsabile del procedimento amministrativo

È la persona che ha la responsabilità del documento, cioè può in parte correggerlo o completarlo. Suo compito è quello di inserire il documento in un fascicolo (cartaceo e informatico) e trattare il procedimento amministrativo nella sua complessità.

5.16 Utente addetto alla struttura aziendale abilitato alla consultazione

Gli utenti (addetti alla struttura AZIENDALE) possono essere abilitati ad accedere al sistema informatico limitatamente ai documenti della rispettiva struttura con le restrizioni formalmente indicate dal Responsabile della struttura complessa compresi fra un livello massimo (tutti i documenti della stessa struttura) e minimo (esclusivamente quelli trattati dalla sede distaccata). In tal senso il Responsabile della struttura complessa deve anche indicare al responsabile del servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi , per ciascun utente (addetto e protocollista) il livello di accesso in modifica (inserimento dati) e in consultazione.

5.17 Registro di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico ogni evento deve essere registrato su un supporto alternativo (informatico o analogico nel caso di mancanza di corrente elettrica), denominato *Registro di emergenza* (RE).

Su questo registro devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico.

Nel concreto, il PROTOCOLLO GENERALE utilizzerà un Registro cartaceo, all'uopo predisposto ove dovrà essere riportato un numero cardinale sequenziale di due cifre o più cifre, da RE (Registro di emergenza); ad esempio, RE01, RE02, etc. .

Prima di autorizzare l'avvio della procedura, il responsabile del servizio di protocollo informatico dovrà darne formale comunicazione al Direttore Generale dell'.A.S.L. e dovrà compilare il registro per la sua attivazione riportando data e ora dell'attivazione stessa..

Ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno. La numerazione del registro, qualora sia utilizzato più volte durante l'anno, sarà comunque progressiva per consentire l'univoca identificazione del documento sull'anno di riferimento.

Il responsabile del servizio di protocollo informatico dovrà annotare nel protocollo di emergenza i periodi di attivazione del registro di emergenza. Qualora nel corso di un anno non si sia fatto ricorso al registro di emergenza, deve annotarne anche il mancato uso.
Ogni documento è individuato dal numero assegnato nel registro di emergenza, anno e data di registrazione, individuazione strutture competenti e per conoscenza.
Una volta ripristinata la piena funzionalità del sistema di protocollo unico, il responsabile del protocollo riserverà nelle date di protocollazione di emergenza il numero complessivo di numeri di protocollo risultanti sul registro di emergenza. Il protocollo generale recupererà conseguentemente i documenti presenti sul registro di emergenza ai quali sarà attribuito un secondo numero di protocollo generale e nelle annotazioni sarà inserito il numero attribuito nel registro di emergenza..
Contestualmente sarà possibile utilizzare correttamente il sistema per attribuire in tempo reale la numerazione di protocollo ai documenti in arrivo e partenza del momento.
Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio. A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recheranno, pertanto, due numeri: uno del protocollo di emergenza (che sarà contenuto nelle annotazioni) e uno del protocollo unico. L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo; l'efficienza, invece, verrà garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica (qualora attivata)

Parte Sesta

6 la classificazione e fascicolazione dei documenti

6.1 Classificazione dei documenti

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario di Classificazione che sarà a breve ridottato . la classificazione dei documenti sia in arrivo che in partenza è demandata ai Responsabili di Procedimento delle singole strutture aziendali non appena sarà approvato il nuovo titolario di classificazione e saranno formati gli operatori.

6.2 Fascicolazione dei documenti - Formazione ed identificazione dei fascicoli

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentarie.
L'apertura di un nuovo fascicolo è effettuata dal Responsabile del procedimento (o suo delegato) attraverso la registrazione sul repertorio/elenco dei fascicoli e nel sistema informatico delle seguenti informazioni:
a) titolo, classe e sottoclassi del Titolario di classificazione;
b) numero del fascicolo (la numerazione dei fascicoli è annuale per ogni classe);
c) oggetto del fascicolo;
d) data di apertura;
e) assetto a cui è assegnato;
f) responsabile del procedimento;
g) livello di riservatezza;
h) tempo di conservazione.
I) elenco dei documenti contenuti

6.3 Processo di formazione dei fascicoli

In presenza di un documento da inserire in un fascicolo, il Responsabile del procedimento stabilisce, consultando le funzioni del sistema informatico o il repertorio dei fascicoli e sulla base dei criteri generali indicati nell'allegato, se esso si collochi nell'ambito di un fascicolo già aperto o se debba essere creato un fascicolo nuovo.
Qualora si riceva un documento analogico da inserire in un fascicolo informatico, sarà cura del Responsabile del procedimento produrre, se del caso, la copia digitale conforme del documento stesso, in ottemperanza alle norme in materia di riproduzione sostitutiva.
I documenti prodotti dall'Azienda (interni e in partenza) sono fascicolati da chi li scrive, che provvede all'inserimento del documento nel fascicolo corrispondente.
I codici alfanumerici di fascicolazione sono riportati su tutti i documenti.
Qualora il fascicolo sia composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti, l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione ed il numero di repertorio.

6.4 Modifica delle assegnazioni dei fascicoli

La riassegnazione di un fascicolo è effettuata dal Responsabile del procedimento che ha in carico il fascicolo, provvedendo a correggere le informazioni del sistema informatico e del repertorio dei fascicoli ed inoltrando successivamente il fascicolo al Responsabile del procedimento di nuovo carico.

Delle operazioni di riassegnazione è lasciata traccia nel sistema informatico di gestione dei documenti.

6.5 Tenuta dei fascicoli dell'Archivio corrente

I fascicoli dell'Archivio corrente sono gestiti a cura dei Responsabili dei vari assetti e, qualora cartacei, conservati presso gli uffici di competenza fino al trasferimento nell'Archivio di deposito.
Per quanto riguarda i fascicoli informatici, il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, d'intesa con il Responsabile della Conservazione dei documenti informatici, provvede al loro trasferimento in archivi informatici di conservazione.
In alternativa, il Responsabile della Conservazione, d'intesa con il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, avvia le opportune iniziative per l'affidamento in *outsourcing* del servizio di conservazione, in conformità alle normative vigenti.

PARTE SETTIMA

7 La conservazione dei documenti

7.1 Struttura dell'archivio

L'Archivio è suddiviso funzionalmente in Archivio corrente, Archivio di deposito e Archivio Storico.

► Per ***Archivio corrente*** si intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale e contingente.

L'Archivio corrente è organizzato presso ciascun assetto o struttura aziendale, a cura e sotto la responsabilità del Dirigente ad essa preposto, il quale provvede ad assicurarne l'ordinata conservazione e la corretta gestione.

► Per ***Archivio di deposito*** si intende il complesso dei fascicoli relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico.

L'Archivio di deposito è finalizzato a conservare i documenti non necessari alle attività correnti per il tempo necessario a garantire l'assolvimento degli obblighi di natura amministrativa e giuridica e per procedere alle operazioni di selezione e scarto prima del versamento nell'Archivio storico.

► Per ***Archivio Storico*** si intende il complesso dei documenti relativi ad affari esauriti da oltre quaranta anni e destinati, previa effettuazione delle operazioni di selezione e scarto, alla conservazione permanente.

L'Archivio Storico si implementa delle eventuali future acquisizioni di materiale archivistico dell'Azienda o di altri fondi provenienti da Enti pubblici soppressi o da privati, sia per acquisto sia per donazione o comodato.

L'Archivio Storico svolge le seguenti funzioni e persegue le seguenti finalità:

a) la conservazione, l'ordinamento e la gestione dei fondi archivistici costituenti la memoria storica dell'Azienda;

b) la consultazione e la fotoriproduzione dei documenti in esso conservati, su richiesta dei soggetti che ne abbiano interesse;

c) la promozione di attività didattiche e di ricerca storica, nonché di valorizzazione dei patrimoni documentari in esso contenuti;

d) il raccordo costante con l'Archivio di deposito.

7.2 Responsabilità della conservazione dei documenti

La responsabilità della conservazione e della custodia dei documenti (di natura amministrativa/istituzionale, sanitaria/clinica, socio-sanitaria) degli Archivi correnti e di quelli presenti in eventuali depositi provvisori (ossia i cui documenti non sono formalmente riversati) nell'Archivio di deposito è affidata ad ogni dirigente responsabile dell'assetto presso cui sono prodotti/acquisiti i documenti.

L'accesso ai documenti degli archivi correnti è assicurato in conformità al Regolamento aziendale tenuto conto della Legge 241/1990, del DPR n. 184/2006, della L.R. n. 1/2012 e del dlgs 196/2003.

7.3 Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione (di protocollo o altro strumento di registrazione) e conservati nell'archivio informatico della procedura gestionale ARCHIFLOW. Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello *scanner*, sono memorizzate nel sistema al termine del processo di scansione.

7.4 Conservazione dei documenti informatici

Il Responsabile della Conservazione dei documenti informatici, d'intesa con il Responsabile del Trattamento dei Dati e con il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, in collaborazione con l'assetto aziendale preposto alla gestione informatica e con il supporto della tecnologia disponibile, provvede:

- a conservare i documenti informatici;
- a controllare periodicamente a campione la leggibilità dei documenti stessi;
- a salvaguardare gli strumenti di descrizione, ricerca, gestione e conservazione dei documenti.

Va in ogni caso garantita la conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi, in conformità alle norme vigenti in tema di conservazione sostitutiva.

La documentazione prodotta nell'ambito del Manuale di gestione e dei relativi aggiornamenti deve essere conservata integralmente e perennemente nell'Archivio dell'Azienda.

7.5 Selezione dei documenti

Almeno una volta l'anno in base al massimario di scarto in fase di revisione viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale con l'invio della richiesta di autorizzazione allo scarto alla Soprintendenza Archivistica.

ALLEGATO 1 dell'allegato A alla deliberazione n. 357 del 14 OTTOBRE 2015

NORMATIVA DI RIFERIMENTO

Decreto del Presidente della Repubblica n. 128 del 27 marzo 1969 - Ordinamento interno dei servizi ospedalieri.

Legge 7 agosto 1990, n. 241 e ss. mm. e ii. - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 - Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.

Decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 - Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche.

Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513.

Direttiva del Presidente del Consiglio dei Ministri 28 ottobre 1999 - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni.

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.

AIPA Deliberazione n. 51/2000 del 23 novembre 2000 - Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss. mm. e ii. - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

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

Decreto Legislativo 23 gennaio 2002, n. 10 - Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

Ministro per l'innovazione e le tecnologie - 9 dicembre 2002 - Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

Decreto del Presidente della Repubblica 7 aprile 2003, n. 137 - Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10.

Decreto Legislativo 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali.

Ministro per l'innovazione e le tecnologie - 14 ottobre 2003 - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi.

Dipartimento per l'innovazione e le tecnologie - Direttiva 27 novembre 2003 - Impiego della posta elettronica nelle pubbliche amministrazioni.

Direttiva del Ministero per l'Innovazione e le Tecnologie 19 dicembre 2003 - "Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche Amministrazioni.

CNIPA Deliberazione 19 febbraio 2004, n.11 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

Decreto Legislativo 22 gennaio 2004 n. 42 - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.

Decreto Legislativo 7 marzo 2005, n. 82 e ss. mm. e ii. - Codice dell'amministrazione digitale (CAD).

CNIPA Circolare 6 settembre 2005, n.48 - Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Decreto Legislativo 4 aprile 2006, n.159 - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.

Decreto Legislativo 24 marzo 2006, n.156 - Disposizioni correttive ed integrative al decreto legislativo 22 gennaio 2004, n.42, in relazione ai beni culturali.

Decreto Legge 29 novembre 2008 n. 185 – art. 16 c. 6 convertito in Legge 28 gennaio 2009 n. 2 - Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale - relativo all'utilizzo della posta elettronica certificata.

Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.

CNIPA - Linee guida per l'utilizzo della firma digitale – Versione 1.3 - Aprile 2009.

CNIPA Deliberazione 21 maggio 2009, n. 45 - Regole per il riconoscimento e la verifica del documento informatico.

Deliberazione Garante per la Protezione dei dati personali del 2 marzo 2011, n. 88 - Linee Guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.

Regole tecniche DigitPA per la consultazione ed estrazione di indirizzi PEC ed elenchi di indirizzi PEC di cui all'art. 6 comma 1-bis del CAD - 22 aprile 2011.

Decreto del Presidente del Consiglio dei Ministri 22 luglio 2011 - Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del CAD.

CIRCOLARE DigitPA 1 dicembre 2011, n. 58 - Attività di DigitPA e delle Amministrazioni ai fini dell'attuazione degli adempimenti previsti dall'articolo 50 -bis (Continuità Operativa) del «Codice dell'Amministrazione Digitale» (D.lgs. n. 82/2005 così come modificato dal D.lgs. 235/2010).

Decreto Legge 9 febbraio 2012 n. 5 convertito nella Legge 4 aprile 2012, n. 35 - Disposizioni urgenti in materia di semplificazione e di sviluppo.

Decreto Legge 22 giugno 2012, n. 83 (cosiddetto "Decreto Sviluppo"), convertito con modificazioni, dalla Legge 7 agosto 2012, n. 134 (in particolare: Art. 19 Istituzione dell'Agenzia per l'Italia digitale).

Decreto del Presidente del Consiglio dei Ministri 6 settembre 2012 - Separati certificati di firma, ai sensi dell'art. 28, comma 3-bis), del CAD, di cui al D.L. 7 marzo 2005 n. 82.

Deliberazione Garante per la Protezione dei dati personali 11 ottobre 2012 n. 280 - Protocollo informatico e protezione dei dati personali dei lavoratori.

Decreto Legge n. D.L. 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese - **convertito in Legge 17 dicembre 2012, n. 221** – art. 5, 12, 13 e 13 bis.

Agenzia per l'Italia Digitale - Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni – Aggiornamento 2013

Circolare Agenzia per l'Italia Digitale n. 60 del 23 gennaio 2013 - Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni.
Revisione della Circolare AIPA del 7 maggio 2001, n. 28 relativa agli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati, ai sensi dell'art. 18, comma 2, del D.P.C.M. 31 ottobre 2000 di cui al D.P.R. 28 dicembre 2000, n. 445.

Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

D.M. 19 marzo 2013 - Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (INI-PEC).

Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013 - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.

Circolare Agenzia per l'Italia Digitale n. 61 del 29 marzo 2013 - Disposizioni del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, 221 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle Pubbliche Amministrazioni.

Circolare Agenzia per l'Italia Digitale n. 62 del 30 aprile 2013 - Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD.

Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013 - Modalità di consegna, da parte delle Aziende Sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d) numeri 1) e 2) del decreto-legge13 maggio 2011, n. 70, convertito con modificazioni, dalla legge 12 luglio 2011, n. 106, recante "Semestre europeo – prime disposizioni urgenti per l'economia".

Decreto del Presidente del Consiglio dei Ministri 23 agosto 2013, n. 109 - Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR).

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

SOC I.C.T.
Gestione delle Tecnologie Informatiche di Comunicazione e del Sistema Informativo
Sede legale :Via Mazzini, 117 – 28887 Omegna (VB)
Sede Operativa Omegna
Tel. 0323868202-03 Fax 0323 868220
e-mail :ict@aslvco.it

ALLEGATO 2 dell'allegato A alla deliberazione n. 357 del 14 OTTOBRE 2015

1. INTRODUZIONE

Nello svolgimento delle funzioni specifiche delle Pubbliche Amministrazioni, ed in particolare della Sanità, è sempre più importante il supporto informatico, che consente un netto miglioramento dei servizi erogati ai cittadini.
Questo aspetto comporta che, per assicurare in modo corretto l'erogazione dei servizi, sia di primaria importanza la continuità di funzionamento dei sistemi informatici.
A tale proposito, l'articolo 50-bis del CAD aggiornato (che riguarda proprio la "Continuità operativa") delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni, a DigitPA e al Ministro:

- In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le p.p.a.a. predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività.
- Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.
- A tali fini, le pubbliche amministrazioni definiscono:
  - **a.** il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
  - **b.** il piano di Disaster Recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.
  - **c.** I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

1.1 Obiettivo del documento

In ottemperanza a quanto citato nel punto 4 dell'articolo 50-bis del CAD viene redatto il presente documento di SFT nel quale, oltre ad evidenziare quanto emerso nel percorso di autovalutazione, vengono anche evidenziati:

- gli eventuali scostamenti tra la soluzione individuata e quella scelta dalla Amministrazione;
- le modalità ed i tempi per adottare la soluzione individuata al termine del percorso di autovalutazione e per allinearsi a quanto previsto dalle Linee Guida.

Questo documento si propone, quindi, di fornire a DigitPA le informazioni relative alla completa realizzazione del piano di disaster recovery, come parte integrante di un più ampio piano di continuità operativa che non interessa solo la parte informatica.

2. INFORMAZIONI GENERALI

Nome Amministrazione	ASL VCO
Sede centrale (città):	Omegna (VB)
Settore di attività	Azienda Sanitaria Locale
Responsabile CO/DR:	Dott.ssa Anna GAGLIARDI
AOO (Area Org. Omog.)/ENTE	ASL VCO
Indirizzo PEC per le comunicazioni	protocollo@pec.aslvco.it

L'**ASL VCO** è azienda sanitaria inserita organicamente nel Servizio Sanitario Regionale del Piemonte con la finalità di proteggere, promuovere e migliorare la salute della popolazione residente mediante programmi e azioni coerenti con i principi e con gli obiettivi indicati dalla pianificazione sanitaria e socioassistenziale nazionale e regionale.
La missione dell' Azienda è rispondere ai bisogni ed alle aspettative di salute dei cittadini gestendo con efficienza le risorse disponibili per garantire prestazioni di prevenzione, cura e riabilitazione efficaci e appropriate, offerte con tempestività, rispetto della persona ed in condizioni di sicurezza.
Per rispondere alla propria missione l'Azienda opera anche in collaborazione e alleanza con altri soggetti privati e pubblici, operando con trasparenza e favorendo la partecipazione dei cittadini nella definizione delle scelte e nella valutazione dei risultati.
L'Azienda persegue inoltre la valorizzazione del proprio capitale di tecnologie e di professionisti come competenze distintive dedicate alla gestione e produzione di servizi sanitari

L'Azienda Sanitaria, che presenta un'**estensione territoriale di circa 2.300 km quadrati**, per il 96% montani, ed una densità abitativa media di 74 abitanti/Kmq., comprende 84 Comuni, per un totale di 174.036 abitanti, gestisce:
Un OSPEDALE UNICO PLURISEDE con due Presidi Ospedalieri:
Stabilimento Ospedaliero Castelli di Verbania
Ospedale S. Biagio di Domodossola
Tre Distretti Sanitari Territoriali:
Domodossola
Omegna
Verbania
Le strategie aziendali.

Con la redazione dei Piani aziendali 2006/07 e 2008/10 sono stati delineati nuovi indirizzi strategici con lo scopo di garantire a tutta la popolazione, oltre ad un appropriata ed efficiente assistenza ospedaliera, anche un'efficace azione di prevenzione delle malattie ed un'assistenza territoriale capillare e diversificata. Si è inteso offrire una risposta più idonea ai bisogni dell'utenza secondo il concetto di **assistenza continua** che si sviluppa nei diversi livelli: assistenza domiciliare, assistenza in strutture tutelari (RSA, RAF, Hospice..), assistenza ospedaliera, assistenza post-ospedaliera, assistenza domiciliare.

Le strategie individuate a livello aziendale sono le seguenti:

- **sviluppo delle politiche e delle iniziative di prevenzione e di tutela della salute**;
- **diffusione delle esperienze dei servizi sanitari territoriali** (in particolare, tenuto conto del contesto morfologico del territorio, in prevalenza montano, al fine di offrire risposte adeguate ai bisogni della popolazione si è reso necessario organizzare il sistema sanitario locale con una diffusione capillare dei servizi per garantirli, in modo omogeneo e con pari opportunità di accesso, all'intera popolazione del VCO);
- **riordino degli ospedali di Verbania e Domodossola e realizzazione dell'ospedale integrato plurisede del VCO** funzionante secondo la logica dei percorsi diagnostici terapeutici, dotato di equipes professionali (mediche e chirurgiche) uniche, che agiscono nei diversi presidi che compongono l'ospedale plurisede, presso i quali sono invece collocate, stabilmente, le unità di degenza e le equipes di assistenza infermieristica alla persona;
- **riorganizzazione dell'azienda secondo logiche di processo** per assicurare la presa in carico del paziente ed il suo inserimento in ben definiti e normati percorsi assistenziali.

Tali strategie si pongono la finalità di porre il cittadino/paziente, con le sue istanze e bisogni, al centro dell'attenzione, garantendo la sua presa in carico.

Figura 1: Rappresentazione le macro funzioni aziendali e i loro processi

Elenco delle sedi aziendali

Quasi tutte le sedi della ASL VCO sono collegate tramite WAN, attraverso la quale possono afferire alle risorse ICT, a seconda delle competenze svolte.

Le sedi collegate sono:

- o Direzione Generale - Palazzo Beltrami I – Via Mazzini 117 – Omegna
- o Servizi Amministrativi - Palazzo Beltrami II - Via Mazzini 117 – Omegna
- o Stabilimento Ospedaliero "Castelli" - Via Crocetta – Verbania Pallanza.
- o Presidio Ospedaliero " S. Biagio " - Largo Caduti Lager Nazisti n° 1 - Domodossola.
- o C.O.Q. Ospedale " Madonna del Popolo " di Omegna - Via Lungo Lago Buozzi - Omegna.
- o Verbania Viale Sant'Anna n° 83 - Stresa Via De Martini n° 20.
- o Cannobio Piazza Ospedale n° 6.
- o Verbania-Intra Via alla Bolla 2
- o Domodossola Via Scapaccino n° 47
- o Villadossola - Via Bianchi Novello n° 74
- o Pieve Vergonte – Via Massari n° 23
- o Premosello Chiovenda - Via Milano n° 7.
- o Baceno - Via Roma
- o Vanzone San Carlo - Via Gorini n. 20
- o Santa Maria Maggiore - Via Marconi n°61.
- o Varzo - Via Alneda

o Omegna Via Mazzini 96
o Omegna – Vicolo Mergozzolo
o Gravellona Toce - Via Realini n° 36.
o San Maurizio D'Opaglio - Piazza 1° Maggio.
o Omegna Casa dell'Anziano Massimo Lagostina Via Risorgimento 5
o Omegna Via Manzoni n° 31
o Domodossola Via Spezia n° 5
o Verbania Via Crocetta 18
o Verbania – Via Crocetta
o Omegna – Via Lungo Lago Buozzi
o Omegna (Crusinallo) - Via IV Novembre 294

Gruppi di cure primarie

o Cannobio Centro Polifunzionale Via Paolo Zaccheo 16
o M.M.G. Omegna Via Mazzini 97

3. CONTINUITA' OPERATIVA

Il presente documento prende in considerazione i servizi rivolti verso il pubblico, che offrono le proprie funzionalità a utenti finali (cittadini, imprese, altre PA, utenti interni all'Amministrazione) e per la cui erogazione sono utilizzate tecnologie ICT per la gestione dei dati e dei processi interni.
E' importante ricordare che il blocco dei sistemi informatici implica la sospensione del servizio all'utenza solo in pochi casi, che assai raramente impattano sull'obiettivo principale dell'Azienda, cioè la tutela della salute.
Le funzioni svolte dall'informatica nell'ambito dei processi clinici e di erogazione delle prestazioni sanitarie, sono prevalentemente di supporto all'attività sanitaria specifica.
Tuttavia il numero crescente di processi controllati e svolti con l'ausilio di tecnologie informatiche, rende sempre più pressante la necessità di garantire la piena e continua disponibilità degli strumenti ICT, anche mediante un'adeguata infrastruttura di rete dati.
Nell'organizzazione dell'ASL VCO è presente la Struttura Complessa ICT che esercita tutte le funzioni relative al sistema informativo dell'Azienda e gestisce le risorse ed attività finalizzate alla gestione dell'informazione (tecnologie ed infrastrutture, soluzioni applicative, procedure, banche dati). Pur in presenza di un numero limitato di personale tecnico, la SOC ICT è punto di riferimento unico sia per le Strutture interne che per i fornitori delle soluzioni ICT installate presso l'ASL; i carichi di lavoro dovuti alla crescente complessità e alla continua evoluzione del settore, sono un elemento importante per la redazione dei piani di Continuità Operativa (CO) e di Disaster Recovery (DR).

Per quanto riguarda la CO, la Direzione Sanitaria Ospedaliera ed i Responsabili dei Dipartimenti hanno definito specifiche procedure manuali da adottare in ambito clinico nel caso di temporanea indisponibilità del Sistema Informativo (ad es. accettazione ospedaliera, gestione accessi PS/DEA, richieste a Servizi Diagnostici, compilazione di modulistica cartacea, ecc.).

3.1 DISASTER RECOVERY

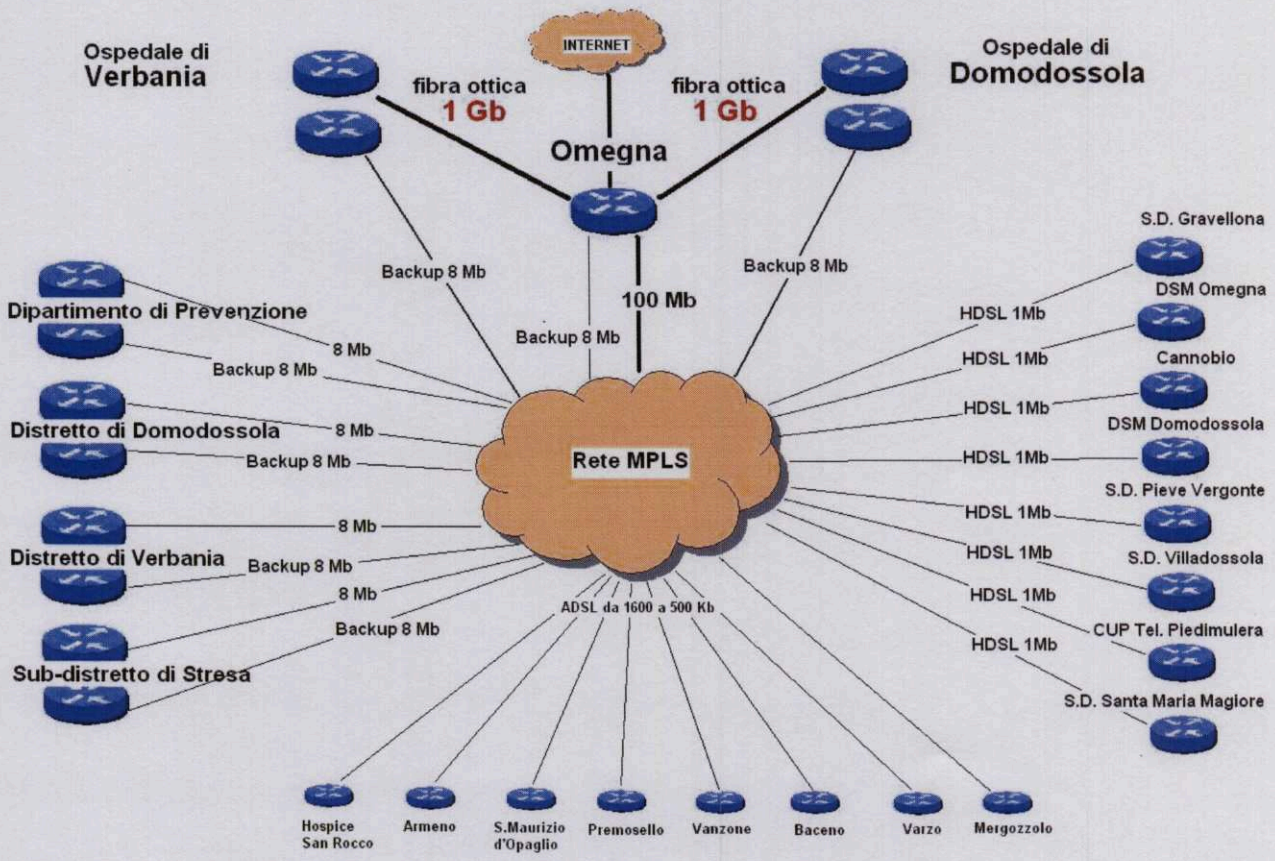
Per quanto riguarda il DR nel 2011 è stato effettuato uno studio di fattibilità che ha permesso di acquisire le componenti hardware e software necessarie alla realizzazione di una struttura che consenta, in caso di gravi problemi, la continuità di servizio o, quantomeno, il ripristino delle condizioni lavorative (compreso il recupero dei dati) nei tempi più brevi possibili.

3.2 INFRASTRUTTURA DI RETE DATI

La ASL VCO è dotata di una rete dati che consente di collegare la maggior parte delle sedi Aziendali mediante collegamenti dimensionati con tipologie e velocità differenti
Le 3 Sedi principali (Direzione Generale di Omegna, Ospedale di Domodossola, Ospedale di Omegna, Ospedale di Verbania) sono dotate di collegamenti in fibra ottica con backup in rame a 8 Mbps.
Le sedi secondarie più importanti (Distretti di Verbania e Domodossola, Dipartimento di Prevenzione, Stresa – Subdistretto e presidio di Dialisi turistica) hanno un collegamento principale in rame a 8 Mbps backuppato con un secondo collegamento in rame, sempre da 8 Mbps.
Le linee di backup vengono attivate automaticamente quando si presenta un problema sui collegamenti principali; al ripristino delle condizioni si riattiva automaticamente il collegamento principale.
Come già precisato, le altre sedi hanno collegamenti dimensionati a seconda delle rispettive esigenze.

Nome sede	Città		Tipo di Link
Sede Centrale (Omegna CED)	Omegna	SDH	Principale
Sede Centrale (Omegna CED)	Omegna	SDH	Principale
Sede Centrale (Omegna CED)	Omegna	MPLS	Backup
Sede Centrale (Omegna CED)	Omegna	DWDM	Principale
Ospedale "Castelli"	Verbania	DWDM	Principale
Ospedale "Castelli"	Verbania	MPLS	Backup
Ospedale San Biagio	Domodossola	DWDM	Principale
Ospedale San Biagio	Domodossola	MPLS	Backup
Sub Distretto Stresa	Stresa	MPLS	Principale
		MPLS	Backup
Dip prevenzione	Omegna	MPLS	Principale
		MPLS	Backup
Distretto Domodossola	Domodossola	MPLS	Principale
		MPLS	Backup
Distretto di Verbania	Verbania	MPLS	Principale
		MPLS	Backup
Sub-distretto Gravellona	Gravellona	MPLS	Principale
CUP Telefonico	Piedimulera	MPLS	Principale
Sede DSM	Omegna	MPLS	Principale
Sub-Distretto Cannobio	Cannobbio	MPLS	Principale
Sub-distretto Pieve Vergonte	Pieve Vergonte	MPLS	Principale

Sub-distretto Villadossola	Villadossola	MPLS	Principale
Sede DSM	Domodossola	MPLS	Principale
Sub-distretto S.Maria Maggiore	S.Maria Maggiore	MPLS	Principale
Ex Ospedale	Premosello Chiovenda	MPLS	Principale
Sub-distretto	Vanzone San Carlo	MPLS	Principale
Sub-distretto	Baceno	MPLS	Principale
Sub-distretto	Varzo	MPLS	Principale
Hospice Verbania Intra	Verbania	MPLS	Principale
Sub-distretto	San Maurizio d'Opaglio	MPLS	Principale
NPI Omegna	Omegna	MPLS	Principale



Questo tipo di infrastruttura ha permesso di duplicare, all'interno di un locale adeguatamente dimensionato e climatizzato, una parte del CED principale, che si trova presso la sede della Direzione Generale a Omegna, con replica dei dati in modalità sincrona.
Le sedi interessate (Direzione Generale – Omegna Via Mazzini 117 e Ospedale Castelli - Verbania Via Fiume) distano circa 20 km. E sono collegate tra loro tramite una dorsale in fibra ottica con backup automatico, in caso di guasto del collegamento principale, su VPN MPLS a 8Mbps.

3.3 SERVIZI EROGATI NELL'AMBITO DELL'ANALISI DEL D.R

Considerato l'elevato numero di servizi erogati dalla ASL si è deciso di procedere con una valutazione per classi di servizio: sono stati raggruppati i servizi omogenei in termini di utenza,

livello di assistenza (Territorio/Prevenzione, Ospedale, Supporto), tempistica di erogazione, infrastruttura ICT.

La seguente tabella elenca e descrive le classi di servizio individuate; alle classi di servizio è stato associato un codice che verrà utilizzato per brevità nelle esposizioni successive.

CLASSE DI SERVIZIO		Criteri di aggregazione	Infrastruttura
Codice	Descrizione		
1 H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale	Utenza esterna, livello Ospedale, erogazione reparti 7X24, erogazione ambulatori 5x10	MS Server – Linux – Oracle - Web
2 H	Procedure Amministrativo sanitarie (CUP, ADT, Anagrafe assistiti, Statistiche, Flussi ecc.)	Utenza esterna, livello Ospedale, erogazione 5X8	MS Server – Oracle – Client Server - Web
3 H	FAID – Gestione DEA	Utenza esterna, livello Ospedale, erogazione 7X24	MS Server – Oracle – Client Server - Web
4 H	Gestione archivi Ospedalieri di specialità	Utenza esterna, livello Ospedale, erogazione 7X24	MS Server – Oracle – Client Server - Web
5 H	DNLAB – Laboratorio Analisi	Utenza esterna/interna, livello Ospedale, erogazione 7X24	MS Server – Oracle – Client Server - Web
6 H	SINCROMED – Radiologia (RIS/PACS)	Utenza esterna, livello Ospedale, erogazione 7X24	MS Server – Oracle – Client Server - Web
7 H	MOSAIQ - Radioterapia	Utenza esterna, livello Ospedale, erogazione 5X8	MS Server – Oracle – Client Server - Web
8 H	SPARTITO – Anatomia e Istologia Patologica	Utenza esterna, livello Ospedale, erogazione 5X12	MS Server – Oracle – Client Server - Web
9 H	ELIOT - SIMT	Utenza esterna, livello Ospedale, erogazione 7X24	Linux – Oracle – Client Server - Web
1 T	Sistema Informativo Territoriale	Utenza esterna, livello Territorio, erogazione 5X8	MS Server – Oracle – Client Server - Web
1 S	Sistema Amministrativo Contabile	Utenza interna, livello Supporto, erogazione 5X8	MS Server - Oracle – SQL – Client Server - Web
2 S	Protocollo	Utenza interna, livello Supporto, erogazione 5X8	Sistema Proprietario – Client Server - Web
3 S	Servizi WEB	Utenza eterogenea, livello Supporto, erogazione 7X24	Web

Cod.	Servizio/classi di servizio	Servizio	Descrizione servizio	Tipologia di utenza
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale. (*) (*) Integrazioni in corso d'opera	Gestione cartella clinica	Gestione integrata storico paziente	Eterogenea
		Consulenze	Gestione richieste consulenze a servizi interni	Eterogenea
		Cartella clinica ospedaliera	Gestione iter prericovero/ricovero	Eterogenea
		Gestione reparto	Gestione spostamenti interni	Utente interno
		Cart. clinica ambulatoriale	Gestione informazioni	Eterogenea
		Richieste laboratorio	Gestione completa richieste esami interni a laboratorio e visualizzazione referti. Integrazione dati strutturati	Utente interno
		Richieste anatomia e istologia patologica	Gestione completa richieste esami interni a anatomia patologica e visualizzazione referti	Utente interno

Cod.	Servizio/classi di servizio	Servizio	Descrizione servizio	Tipologia di utenza
		Richieste radiologia	Gestione completa richieste esami interni a radiologia e visualizzazione referti e immagini	Utente interno
		Cartella RRF	Gestione cartella clinica utenti Recupero e Rieducazione Funzionale	Eterogenea
		Servizi anagrafici	Servizio allineamento anagrafe locale con anagrafe regionale AURA	Utente interno
2H	Procedure amministrativo sanitarie	ADT	Accettazione Ospedaliera, Gestione liste d'attesa degenza	Aziende/cittadini
		CUP	CUP e CUP telefonico	Aziende/cittadini
		Anagrafe Assistiti	Gestione anagrafica integrata	Aziende/cittadini
		Statistiche	Elaborazioni statistiche	Utenti interni
		Flussi	Estrapolazione flussi per Ministero, Regione, ecc.	Utenti interni
3 H	Gestione DEA	FAID	Gestione accessi, consulenze DEA/PS	Aziende/cittadini
4H	Gestione su archivi ospedalieri di specialità	OK-DH oncologico	Gestione cartella DH oncologico	Aziende/cittadini
		MEDWARE - Gestione Nefrologia/Dialisi	Gestione pazienti ricoverati. Gestione pazienti dializzati.	Aziende/cittadini
		Diabetologia	Gestione pazienti diabetici	Aziende/cittadini
		Cytosifo II	Programma per preparazione terapie antiblastiche	Aziende/cittadini
5H	Gestione Laboratorio Analisi	DNLAB – Laboratorio Analisi	Gestione completa Laboratorio Analisi: prenotazione, acquisizione campioni, predisposizione piani di lavoro, produzione referti, collegamento strumenti ecc.	Aziende/cittadini
6 H	Gestione Radiologia (RIS/PACS)	SINCROMED - Gestione Radiologia	Gestione completa attività radiologia: prenotazione, predisposizione piani di lavoro, produzione referti, collegamento strumenti ecc.	Aziende/cittadini
		SYNAPSE - Gestione immagini Radiologia	Sistema PACS (con possibilità di visualizzazione anche nelle sale operatorie, nei Reparti e negli Ambulatori)	Aziende/cittadini
7 H	Gestione Radioterapia	MOSAIQ - Gestione Radioterapia	Gestione cartelle pazienti in radioterapia. Programmazione e gestione strumenti	Eterogenea
8 H	Gestione Anatomia e Istologia Patologica	SPARTITO – Anatomia Patologica	Gestione attività di Anatomia Patoloica	Aziende/cittadini
9 H	Gestione Servizio Immunotrasfusionale (SIMT)	ELIOT - Gestione SIMT	Gestione Servizio Immunotrasfusionale: prenotazione, acquisizione campioni, predisposizione piani di lavoro, produzione referti, collegamento strumenti ecc.	Aziende/cittadini
1T	Sistema Informativo Territorio(*) (*) Alcune funzioni sono in fase di realizzazione.	Gestione Punto Unico Accesso (Punto S)	Gestione Punto S	Aziende/cittadini
		Medicina Sportiva	Gestione pratiche Medicina Sportiva	Aziende/cittadini
		Medicina Integrativa/Protesica	Gestione pratiche prescrizioni e autorizzazioni Medicina Integrativa	Aziende/cittadini
		Gestione ADI	Gestione cartella Assistenza domiciliare	Utente interno
		Gestione UVG	Gestione cartella UVG/UVM (RSA)	Utente interno
		Gestione cartella sociale	Gestione cartella sociale servizi territoriali	Consorzio Servizi Sociali
		Gestione Vaccinazioni	Gestione vaccinazioni	Utente interno
1S	Sistema Amministrativo Contabile	Contabilità Generale	Gestione registrazioni contabili	Utente interno
		Cespiti	Gestione cespiti	Utente interno
		Contabilità Analitica	Gestione contabilità analitica - acqusizione dati - report	Utente interno
		Gestione Entrate	Registrazione fatture attive e gestione reversali	Utente interno

Cod.	Servizio/classi di servizio	Servizio	Descrizione servizio	Tipologia di utenza
		Magazzino Ordini	Gestione movimenti di magazzino e ordini	Utente interno
		Bilanci	Bilanci periodici - chiusure e aperture contabili - stampe	Utente interno
		Richiesta farmaci	Registrazione prescrizioni distribuzione diretta farmaci	Aziende/cittadini
		Rilevazione Presenze	Gestione presenze, assenze, giustificativi personale dipendente	Utente interno
		Gestione credenziali	Gestione credenziali di accesso	Utente interno
2S	Protocollo	Protocollo	Gestione protocollo	Utenti interni
		Delibere	Gestione delibere e determine	Utenti interni
		Posta certificata	Gestione Posta certificata	Utenti interni
		Certificati	Gestione Certificati di malattia	Utenti interni
3 S	Servizi WEB	Gestione servizi web PTW	Servizio collegamento CUP ad applicativo regionale PTW - Pagamenti Ticket Online	Aziende/cittadini
		Sito WEB intranet	Informativa dipendenti	Utenti interni
		Sito WEB	Informativa ASL per il pubblico	Utenti interni/esterni
		Portale dipendente	Distribuzione cedolino on line	Utenti interni

3.4 SERVIZI EROGATI NELL'AMBITO DELL'ANALISI DEL D.R

Per ogni servizio o classe di servizi che fa parte dell'ambito dello Studio di Fattibilità Tecnica è stata redatta una scheda di autovalutazione, i cui risultati sono riportati negli allegati indicati nella successiva tabella:

CLASSE DI SERVIZIO		Allegato	Scheda
Codice	Descrizione		
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale.	Allegato 1	1H_Sistema_Informativo_Ospedaliero
2H	Procedure amministrativo sanitarie	Allegato 2	2H_procedure_amministrativo_sanitarie
3H	Gestione DEA	Allegato 3	3H_Gestione_dea
4H	Gestione su archivi ospedalieri di specialità	Allegato 4	4H_Gestione_archivi-specialistici
5H	Gestione Laboratorio Analisi	Allegato 5	5H Gestione_lab_ana
6H	Gestione Radiologia (RIS/PACS)	Allegato 6	6H_Gestione_Radiologia_(RIS/PACS)
7H	Gestione Radioterapia	Allegato 7	7H_Gestione_Radioterapia
8H	Gestione Anatomia e Istologia Patologica	Allegato 8	8H_Gestiona_anatomia_patologica
9H	Gestione Servizio Immunotrasfusionale (SIMT)	Allegato 9	6H_Gestione_Servizio_Immunotrasfusionale (SIMT)
1T	Sistema Informativo Territorio	Allegato 10	1T_Sistema_Informativo_Territorio
1S	Sistema Amministrativo Contabile	Allegato 11	1S_Sistema_Amministrativo_Contabile
2S	Protocollo	Allegato 12	2S_Protocollo
3S	Servizi WEB	Allegato 13	3S_Servizi_WEB

4 IL RISULTATO DEL PERCORSO DI AUTOVALUTAZIONE

In questo capitolo sono riportati i dati emersi nel corso dell'autovalutazione.

CLASSE DI SERVIZIO		Indici di criticità			Indice complessivo di Criticità	Classe di criticità	Soluzione Tecnologica (Tier)
Codice	Descrizione	Servizio	Organizzazione	Tecnologia			
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale.	7	8	4	6	Alta	4
2H	Procedure amministrativo sanitarie	6	5	5	6	Alta	4
3H	Gestione DEA	6	4	3	5	Media	3
4H	Gestione su archivi ospedalieri di specialità	6	5	4	5	Media	4
5H	Gestione Laboratorio Analisi	7	4	4	6	Alta	4
6H	Gestione Radiologia (RIS/PACS)	9	4	6	7	Alta	5
7H	Gestione Radioterapia	5	3	4	4	Media	4
8H	Gestione Anatomia e Istologia Patologica	6	3	3	5	Media	4
9H	Gestione Servizio Immunotrasfusionale (SIMT)	7	5	4	6	Alta	4
1T	Sistema Informativo Territoriale	6	6	5	6	Alta	4
1S	Sistema Amministrativo Contabile	5	6	4	5	Media	4
2S	Protocollo	5	5	3	4	Media	3
3S	Servizi WEB	5	3	3	4	Media	3

5 SOLUZIONE TECNOLOGICA/TECNICA

Di seguito viene indicato il dettaglio delle azioni adottate per rispondere alle possibili criticità dovute all'utilizzo di tecnologie informatiche nell'espletamento delle attività istituzionali dell'Ente.

5.1 Soluzioni attualmente adottate

CLASSE DI SERVIZIO		Infrastruttura server	Gestione	Cluster	Mirroring	D.R. (*)	Tipologia e cadenza backup	Gruppo di continuità
Codice	Descrizione							
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale.	DB/Application Server su cluster virtualeVMware	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
2H	Procedure amministrativo sanitarie	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
3H	Gestione DEA	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
4H	Gestione su archivi ospedalieri di specialità	DB/Application Server	ICT	NO	Raid 5	PARZIALE	Automatica, giornaliera, centralizzata	SI
5H	Gestione Laboratorio Analisi	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
6H	Gestione Radiologia (RIS/PACS)	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
7H	Gestione Radioterapia	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera,	SI

							centralizzata	
8H	Gestione Anatomia Patologica	DB/Application Server	ICT	NO	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
9H	Gestione Servizio Immunotrasfusionale (SIMT)	DB/Application Server su cluster	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
1T	Sistema Informativo Territorio	DB/Application Server su cluster virtualeVMware	ICT	SI	Raid 5	NO	Automatica, giornaliera, centralizzata	SI
1S	Sistema Amministrativo Contabile	DB/Application Server su cluster	ICT	SI	Raid 5	PARZIALE	Automatica, giornaliera, centralizzata	SI
2S	Protocollo	DB/Application Server su server virtualeVMware	ICT	NO	Raid 5	SI	Automatica, giornaliera, centralizzata	SI
3S	Servizi WEB	DB/Application Server su server virtuale VMware	ICT	NO	Raid 5	SI	Automatica, giornaliera, centralizzata	SI

(*) In fase di implementazione mediante l'utilizzo della struttura precedentemente descritta.

La valutazione dell'esito delle schede di autovalutazione e delle strutture attualmente installate conducono a due soluzioni tecnologiche (Tier 3 e Tier 4), che sono riassunte nella seguente tabella

CLASSE DI SERVIZIO		Infrastruttura server	Esito autovalutazione (Tier)	Soluzione tecnologica (Tier)
Codice	Descrizione			
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale.	DB/Application Server su cluster virtualeVMware	4	4
2H	Procedure amministrativo sanitarie	DB/Application Server su cluster	4	4
3H	Gestione DEA	DB/Application Server su cluster	3	3
4H	Gestione su archivi ospedalieri di specialità	DB/Application Server	4	4
5H	Gestione Laboratorio Analisi	DB/Application Server su cluster	4	4
6H	Gestione Radiologia (RIS/PACS)	DB/Application Server su cluster	5	4
7H	Gestione Radioterapia	DB/Application Server su cluster	4	4
8H	Gestione Anatomia e Istologia Patologica	DB/Application Server	4	4
9H	Gestione Servizio Immunotrasfusionale (SIMT)	DB/Application Server su cluster	4	4
1T	Sistema Informativo Territoriale	DB/Application Server su cluster virtualeVMware	4	4
1S	Sistema Amministrativo Contabile	DB/Application Server su cluster	4	4
2S	Protocollo	DB/Application Server su server virtualeVMware	3	3
3S	Servizi WEB	DB/Application Server su server virtuale VMware	3	3

5.1.1 SOLUZIONE TECNOLOGICA/TECNICA

Come già indicato precedentemente, solo in pochi casi il blocco delle strutture informatiche impedisce l'erogazione all'utenza dei servizio sanitari di emergenza e/o di routine.
Le soluzioni descritte nelle tabelle successive sono in parte già implementate ed in parte da implementare e derivano dall'analisi già effettuata, che ha portato all'acquisizione dell'infrastruttura precedentemente indicata. La virtualizzazione della maggior parte dei server utilizzati ed il relativo salvataggio in modalità sincrona consentono, comunque, di ridurre al minimo i tempi di ripristino dei singoli server e delle relative procedure informatizzate.

SOLUZIONE A Tier 4	
Soluzione tecnica	Risorse elaborative coerenti al sito primario e sempre disponibili su strutture interne e/o di fornitori di servizio esterni RPO=0 RTO=8h
Stato della Soluzione	Implementata parzialmente
Elenco dei servizi del Tier 4 a cui si riferisce questa particolare soluzione	Classi di servizio: 1 H - PHI - Cartella clinica ospedaliera di reparto/ambulatoriale 2 H - Procedure amministrativo sanitarie 4 H - Gestione su archivi ospedalieri di specialità 5 H - Gestione Laboratorio Analisi 6 H - Gestione Radiologia (RIS/PACS) 7 H – Gestione Radioterapia 8 H - Gestione Anatomia Patologica 9 H – Gestione Servizio Immunotrasfusionale (SIMT) 1 T – Sistema informativo territoriale 1 S - Sistema Amministrativo Contabile
Gestione infrastruttura IT del sito di produzione per i servizi afferenti alla soluzione A	**Tutte le classi di servizio:** gestione interna con contratti di assistenza e manutenzione dei fornitori HW, stipulati con SLA compatibili con RTO e RPO della soluzione. Manutenzione e assistenza SW gestione esterna presso società (5gg/8h) e, per le classi attive 7gg/h24, idonea reperibilità.
Gestione della soluzione per il/i sito/i di DR per i servizi afferenti alla soluzione A	Soluzione interna con implementazione (parzialmente già attiva) di idonea struttura presso lo Stabilimento Ospedaliero di Verbania, che dista circa 20 Km. dal CED principale dell'Azienda
Le caratteristiche della/e soluzione/i di DR sono conformi ai paragrafi 6.3, 6.4 e 6.5 delle "Linee guida per il DR delle PA"	Le caratteristiche della soluzione A di DR saranno conformi ai paragrafi 6.3, 6.4 e 6.5 delle "Linee guida per il DR delle PA"
Descrizione dell'organizzazione per la gestione delle emergenze che si intende adottare (per esempio, come indicato nel capitolo 4 delle "Linee guida per il DR delle PA").	L'organizzazione per la gestione delle emergenze si baserà sull'istituzione del "Comitato di gestione della crisi" con attività e compiti estesi alle funzioni di Gruppo di Supporto. Organizzazione comune a tutte le soluzioni.
Trasferimento dati tra siti: quanti dati vengono trasferiti (GB, TB) relativamente ai servizi afferenti alla soluzione	10 TB
Trasferimento dati tra siti: indicare se vengono trasferiti dati sensibili e/o giudiziari relativamente ai servizi afferenti alla soluzione	Dati sensibili
Modalità di trasferimento dati tra siti	Trasmissione ON LINE sincrona, mediante collegamento in fibra ottica con backup in rame a 8 Mbps.
Tipologia di risorsa elaborativa nel sito primario	Mista
Risorse elaborative previste nel sito secondario	Inferiori al sito primario, ma in grado di supportare le emergenze elaborative
Dimensioni dello storage nel sito primario e secondario relativo ai servizi afferenti alla soluzione A	Storage attuale sito primario 20 TB (comune a diversi servizi + 10 TB nel sito secondario

SOLUZIONE A Tier 4	
Connettività del sito DR con eventuali sedi periferiche	Vedi schema di rete Aziendale
Numero minimo di PDL per garantire la funzionalità di servizi offerti	
Organizzazione per la gestione di eventuali emergenze (ad es. Comitato di Crisi); se non comune con tutte le soluzioni previste, indicarlo	E' prevista e sarà comune a tutte le soluzioni.
Condizioni/rischi valutati per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione	La valutazione delle condizioni e dei rischi per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione A, saranno oggetto del Piano di CO e di DR.
Piano di Disaster Recovery	In parte già realizzato.
Piano di Continuità Operativa	Complessivamente, in fase di studio In alcuni casi è già garantita dall'infrastruttura esistente.

SOLUZIONE B Tier 3	
Soluzione tecnica	Risorse elaborative disponibili su strutture di fornitori di servizio esterni in tempi compatibili con RPO =1 giorno – RTO = 1 giorno
Stato della Soluzione	Da adottare
Elenco dei servizi del tier a cui si riferisce questa particolare soluzione	Classi di servizio: 3 H – Gestione DEA 1 S – Protocollo 2 S – Servizi Web
Gestione infrastruttura IT del sito di produzione per i servizi afferenti alla soluzione A	gestione interna con contratti di assistenza e manutenzione dei fornitori HW e SW, stipulati con SLA compatibili con RTO e RPO della soluzione.
Gestione della soluzione per il/i sito/i di DR per i servizi afferenti alla soluzione A	Soluzione interna con implementazione (parzialmente già attiva) di idonea struttura presso lo Stabilimento Ospedaliero di Verbania, che dista circa 20 Km. dal CED principale dell'Azienda
Le caratteristiche della/e soluzione/i di DR sono conformi ai paragrafi 6.3, 6.4 e 6.5 delle "Linee guida per il DR delle PA"	Le caratteristiche della soluzione B di DR saranno conformi ai paragrafi 6.3, 6.4 e 6.5 delle "Linee guida per il DR delle PA"
Descrizione dell'organizzazione per la gestione delle emergenze che si intende adottare (per esempio, come indicato nel capitolo 4 delle "Linee guida per il DR delle PA").	L'organizzazione per la gestione delle emergenze si baserà sull'istituzione del "Comitato di gestione della crisi" con attività e compiti estesi alle funzioni di Gruppo di Supporto. Organizzazione comune a tutte le soluzioni.
Trasferimento dati tra siti: quanti dati vengono trasferiti (GB, TB) relativamente ai servizi afferenti alla soluzione	5 TB
Trasferimento dati tra siti: indicare se vengono trasferiti dati sensibili e/o giudiziari relativamente ai servizi afferenti alla soluzione	Dati sensibili
Modalità di trasferimento dati tra siti	Trasmissione ON LINE sincrona, mediante collegamento in fibra ottica con backup in rame a 8 Mbps
Tipologia di risorsa elaborativa nel sito primario	Mista

SOLUZIONE B Tier 3	
Risorse elaborative previste nel sito secondario	Inferiori al sito primario, ma in grado di supportare le emergenze elaborative
Dimensioni dello storage nel sito primario e secondario relativo ai servizi afferenti alla soluzione B	Storage attuale sito primario 20 TB (comune a diversi servizi) + 10 TB nel sito secondario. La struttura è comune a quella della soluzione A
Connettività del sito DR con eventuali sedi periferiche	Vedi schema rete aziendale
Numero minimo di PDL per garantire la funzionalità di servizi offerti	
Organizzazione per la gestione di eventuali emergenze (ad es. Comitato di Crisi); se non comune con tutte le soluzioni previste, indicarlo	E' prevista e sarà comune a tutte le soluzioni.
Condizioni/rischi valutati per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione	La valutazione delle condizioni e dei rischi per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione B, saranno oggetto del Piano di CO e di DR.
Piano di Disaster Recovery	In parte già realizzato.
Piano di Continuità Operativa	Complessivamente, in fase di studio In alcuni casi è già garantita dall'infrastruttura esistente.

5.1.2 RIEPILOGO SERVIZI, CRITICITÀ, SOLUZIONE

Nella seguente tabella per ogni servizio/classe di servizi incluso nell'ambito SFT sono riportati il Servizio/classe di servizi, la Classe di criticità, la soluzione tecnologica minima, le soluzioni individuate e l'indicazione di presenza o meno della soluzione.

CLASSE DI SERVIZIO		Classe di criticità	Soluzione tecnologica minima da autovalutazione (Tier)	Soluzione tecnologica individuata	Soluzione tecnologica individuata
Codice	Descrizione				
1H	PHI - Cartella clinica ospedaliera di reparto/ambulatoriale.	Alta	Tier 4	Tier 4 – soluzione A	parziale
2H	Procedure amministrativo sanitarie	Alta	Tier 4	Tier 4 – soluzione A	parziale
3H	Gestione DEA	Media	Tier 3	Tier 3 – soluzione B	parziale
4H	Gestione su archivi ospedalieri di specialità	Alta	Tier 4	Tier 4 – soluzione A	parziale
5H	Gestione Laboratorio Analisi	Alta	Tier 4	Tier 4 – soluzione A	parziale
6H	Gestione Radiologia (RIS/PACS)	Alta	Tier 5	Tier 4 – soluzione A	parziale
7H	Gestione Radioterapia	Alta	Tier 4	Tier 4 – soluzione A	parziale
8H	Gestione Anatomia Patologica	Alta	Tier 4	Tier 4 – soluzione A	parziale
9H	Gestione Servizio Immunotrasfusionale (SIMT)	Alta	Tier 4	Tier 4 – soluzione A	parziale
1T	Sistema Informativo Territorio	Media	Tier 4	Tier 4 – soluzione A	parziale
1S	Sistema Amministrativo Contabile	Alta	Tier 4	Tier 4 – soluzione A	parziale
2S	Protocollo	Media	Tier 3	Tier 3 – soluzione B	parziale
3S	Servizi WEB	Media	Tier 3	Tier 3 – soluzione B	parziale

Conclusioni ed adeguatezza della Soluzione

Sulla base dell'autovalutazione e dell'analisi delle criticità, basata anche sull'esperienza di gestione quotidiana dell'infrastruttura informatica, si ritiene che le soluzioni individuate, oltre ad essere coerenti con i risultato dell'autovalutazione, siano conformi ai livelli di criticità dei servizi erogati.
In particolare la scelta di due soluzioni differenziate per i diversi ambiti, risponde alle necessità di continuità dei servizi ospedalieri, caratterizzati da elevata integrazione dei processi e diffuso utilizzo delle tecnologie informatiche a supporto dell'attività diagnostica, e garantisce comunque ai restanti settori un livello adeguato.

ALLEGATO 3 all'allegato A alla deliberazione n..... del.....

DOCUMENTI IN ARRIVO DALL'ESTERNO CHE POSSONO ESSERE PROTOCOLLATI IN ARRIVO DALLE STRUTTURE COMPETENTI:

DIPARTIMENTO DI PREVENZIONE

- astensione anticipata per gravidanza

DIREZIONE SANITARIA OSPEDALIERA

- Fabbisogno mensile prestazioni infermieristiche da parte delle case di cura convenzionate (generalmente sono comunicazioni che pervengono via fax)
- Resoconto prestazioni infermieristiche rese
- Richiesta copia cartelle cliniche
- Richieste diverse formulate da Organi Giudiziari (Procura, Carabinieri ecc.)
- Attestazioni da parte di Comuni diversi di ricevimento dichiarazioni atti di nascita
- Richieste da parte di ditte diverse per effettuazione esami D.Lgs. 81/2008.
- Comunicazioni varie dei medici specialisti ambulatoriali interni relative alla loro attività ed ai loro dati personali

SOC MEDICINA E CHIRURGIA D'URGENZA

- richieste dell'Autorità Giudiziaria consegnate a mano