Azienda Ospedaliera
Istituto Ortopedico
GAETANO PINI

Deliberazione n. 540	Del - 4 DIC. 2015	Atti 26/2013

Oggetto: ADOZIONE DEL PIANO DI DISASTER PLAN INFORMATICO

IL DIRETTORE GENERALE

premesso

- che la Pubblica Amministrazione deve assicurare la continuità operativa dei propri servizi per garantire il corretto svolgimento delle attività del Paese, anche in presenza eventi imprevisti, ai quali si è finora fatto fronte, generalmente, ricorrendo a soluzioni di emergenza di tipo tradizionale (spostamento di personale tra uffici, attivazione di procedure manuali in sostituzione di quelle informatiche temporaneamente sospese, ecc.);
- che la crescita progressiva dell'utilizzo delle tecnologie informatiche ha reso obbligatorio per le Pubbliche Amministrazioni la definizione di un piano di continuità operativa, cioè l'insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compreso gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso;

visti

1) il D.Lgs. 7 marzo 2005 n. 82 recante il "Codice dell'Amministrazione Digitale" come modificato dal d.lgs. 235/2010 e in particolare l'art. 50 bis che attiene alla "Continuità Operativa" che:
   a) al comma 1 dispone: "In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività"
   b) al comma 3 dispone che le Pubbliche Amministrazioni definiscono:
      i) 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, tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive"
      ii) il Piano di Disaster Recovery che costituisce parte integrante di quello di continuità operativa 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;

Deliberazione n. 540	Del 4 DIC. 2015	Atti 26/2013

c) le "Linee Guida alla Continuità operativa nella Pubblica Amministrazione" – linee guida CNIPA 2006;
d) la circolare DigitPA 1 dicembre 2011 n. 58;
e) la nota 19 aprile 2012 del Direttore Generale Sanita della Regione Lombardia

richiamata:

- la delibera n. 29 del 29 gennaio 2013 con la quale si è costituito il Comitato di Gestione della Crisi ai sensi dell'art. 50 bis del D.Lgs. 82/2005 "Codice dell'Amministrazione Digitale" come modificato dal d.lgs. n, 253/2010;
- la delibera n. 391 del 24 ottobre 2013 con la quale sono stati costituiti i Gruppi Operativi di Supporto al Comitato di Gestione della Crisi;

dato atto

- che ai sensi delle disposizioni normative sopra citate, l'Azienda Ospedaliera ha provveduto alla definizione del Piano di Continuità Operativa che fissa gli obiettivi e i principi da perseguire e descrive le procedure per la gestione della continuità operativa, sottoponendolo alla preventiva valutazione di Lombardia Informatica, l'Ente individuato da Regione Lombardia per le tematiche IT e alla successiva validazione da parte di DigitPA;
- che la Regione Lombardia, coerentemente con le "Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni" ha inteso definire un Piano di Disaster Recovery unico e comune a tutti gli Enti Sanitari Pubblici della Regione Lombardia presentando un unico studio di fattibilità tecnica aggregante tutte le aziende sanitarie pubbliche regionali e sottoponendolo al parere di DigitPA;

preso atto

- del parere espresso con mail del 10 dicembre 2012, depositato agli atti, da Lombardia Informatica sul Piano di Continuità Operativa presentato dalla Azienda Ospedaliera che è risultato coerente con le linee guida regionali;
- del parere favorevole espresso da DigitPA che ha ritenuto coerente il Piano di Disaster Recovery presentato dalla Regione Lombardia;
- dell'adesione da parte dell'Azienda Ospedaliera all'iniziativa regionale per il Distaster Recovery

ritenuto in attuazione delle disposizioni normative sopra richiamate di procedere all'adozione del Piano Aziendale di Disaster Plan informatico come previsto dall'art. 50 bis del d.lgs. n. 82/2005 come modificato dal

Deliberazione n. 540	Del - 4 DIC. 2015	Atti 26/2013

d.lgs. n. 235/2010, allegato al presente provvedimento che ne diventa parte integrante e sostanziale;

verificato che dal presente provvedimento non derivano oneri diretti, né impegni finanziari futuri a carico dell'Azienda Ospedaliera;

visti i pareri favorevoli espressi, per quanto di rispettiva competenza, dal Direttore Amministrativo e dal Direttore Sanitario, ai sensi degli artt. 3 e 3bis del d.lgs. 502/92 s.m.i.;

D E L I B E R A

per i motivi di cui in premessa che qui si intendono integralmente trascritti:

1) di adottare il Piano Aziendale di Disaster Plan informatico allegato al presente provvedimento di cui forma parte integrante e sostenziale;

2) di incaricare i Gruppi Operativi di supporto al Comitato di Gestione della Crisi di procedere alla stesura del Piano di Continuità Operativa;

3) di dare pubblicità al presente argomento (come indicato nell'oggetto della deliberazione) sul sito internet aziendale nell'ambito dei dati della sezione "Amministrazione Trasparente", ai sensi del D.Lgs. 14 marzo 2013 n. 33;

4) di dichiarare il presente provvedimento non soggetto a controllo preventivo, ai sensi dell'art. 18, comma 7, della L.R. n. 33/2009;

5) di disporre la pubblicazione della presente determinazione, dando atto che la stessa è immediatamente esecutiva, ai sensi dell'art. 18 comma 9 della L.R. n. 33/2009.

IL DIRETTORE GENERALE
(dott. Amedeo Tropiano)

CON I PARERI FAVOREVOLI DI COMPETENZA DEL

DIRETTORE AMMINISTRATIVO
(dott. Renato Malaguti)

DIRETTORE SANITARIO
(dott. Nunzio A. Buccino)

S.C./S.S. _____
Si attesta la regolarità amministrativa e tecnica del presente provvedimento.
Responsabile del Procedimento: Ing. Francesca De Giorgi
Pratica trattata da: Rossati Nadia

Azienda Ospedaliera
Istituto Ortopedico
GAETANO PINI

Deliberazione n. 540	Del - 4 DIC. 2015	Atti 26/2013

RELAZIONE DI PUBBLICAZIONE

Si certifica che la presente deliberazione é pubblicata all'Albo Pretorio online di questa Azienda Ospedaliera, per rimanervi affissa per quindici giorni consecutivi.

Milano, lì - 4 DIC. 2015

S.C. AFFARI GENERALI E LEGALI
L'ASSISTENTE AMMINISTRATIVO
(Maria Cianchella)

L'atto si compone di n. 28 pagine, di cui n. 24 pagine di allegati parte integrante.

Azienda Ospedaliera
Istituto Ortopedico
GAETANO PINI
Piazza A. Cardinal Ferrari, 1
20122 Milano - Tel. 02 582961

Polo Riabilitativo
Via Isocrate, 19 - 20126 Milano
www.gpini.it - Part. IVA 00903310159 - Cod. Fisc. 80064670153

Disaster Plan Informatico

0	-	Prima emissione		
Rev.	n°0	Descrizione modifica	Firma	Data

Preparato (data e firma)	Verificato (data e firma)	Approvato (data e firma)
Barbara Savy 30/10/2015	Ponziano Ricciardelli 20/11/2015	Francesca De Giorgi 30/11/2015

Indice

1 Piano di Continuità Operativa ICT e Disasterplan

L'obiettivo del Piano di Continuità Operativa ICT (nel seguito, semplicemente PCO) è quello di definire l'organizzazione, le procedure, le soluzioni tecniche che permettano all'Amministrazione di ripristinare, in caso di interruzioni di qualunque natura, i propri servizi ICT.
Il Piano di Continuità Operativa ICT ha la finalità di:

- Gestire un completo e definitivo ripristino dell'operatività in caso di disastro;
- Reagire agli eventi nel modo più tempestivo possibile;
- Stabilire un flusso di comunicazione efficiente in tempi brevissimi in caso di emergenza

In sostanza il Piano di continuità operativa fissa gli obiettivi da perseguire per garantire la continuità operativa, descrivendone le procedure (interne o affidate a soggetti esterni) ed analizzando tutte le possibili criticità, relative a risorse umane e/o tecnologiche, e proponendo possibili azioni preventive.
Il **Disaster Plan Informatico**, parte integrante del Piano di Continuità Operativa ICT, definisce altresì le misure tecniche ed organizzative atte a garantire il corretto funzionamento dei data center e degli applicativi in siti alternativi a quello di produzione.

1.1 Definizioni e abbreviazioni

Acronimo	Descrizione Estesa
AgID	Agenda per l'Italia Digitale
BIA	Business Impact Analysis
EPR	Electronic Patient Record
FSE	Fascicolo Sanitario Elettronico
PACS	Picture Archiving and Communication System
PCO	Piano di Continuità Operativa
PDR	Piano di Disaster Recovery
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFT	Studio Fattibilità Tecnica
SLA	Service Level Agreement
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
NOC	Network Operation Center
PRI	Piattaforma regionale di integrazione

1.2 Riferimenti

[1] http://www.camera.it/parlam/leggi/deleghe/05082dl.htm
[2] AGID - Linee Guide per il Disaster Recovery delle Pubbliche Amministrazioni

1.3 Destinatari

I destinatari del Piano di Continuità Operativa ICT e del Disaster Plan Informatico sono:

- Direzione strategica
- Il responsabile della Continuità Operativa ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011
- Il comitato di crisi dell'azienda ospedaliera

1.4 Percorso di Fattibilità presso AGID

L'Azienda Ospedaliera "Istituto Ortopedico Gaetano Pini" , in data 30 settembre 2015 ha manifestato la volontà di aderire , al servizio di Disaster Recovery presso il Data Center Regionale di Lombardia Informatica, a conclusione del percorso avviato e condotto da Lombardia Informatica attraverso l'istituzione del gruppo di Lavoro "Disaster Recovery e Continuità Operativa".
Lombardia Informatica ha raccolto l' adesione da parte delle Aziende sanitarie lombarde ed ha richiesto ed ottenuto parere favorevole da parte dell' AGID relativamente alla soluzione di Disaster Recovery progettata

1.4.1 I servizi in ambito ospedaliero supportati da infrastruttura ICT

Le infrastrutture ICT sono parte integrante del processo di erogazione dei servizi di un'azienda sanitaria Per quanto concerne in particolare i servizi erogati da un'azienda ospedaliera, essi si possono differenziare per la loro classe di criticità e livello di "Tier", secondo la classificazione AGID.

Per poter definire un valore che possa aiutare l' Azienda Ospedaliera a valutare in forma sintetica il livello di tolleranza dei propri servizi nei confronti della loro eventuale indisponibilità sono stati individuati specifici indicatori lungo diverse direttrici.

E' possibile individuare un indicatore di sintesi (Indicatore complessivo di criticità), che identifica il livello di criticità dei servizi.
I suddetti livelli di criticità vengono raggruppati in 4 Classi: Bassa, Media, Alta e Critica.

- Critica
  L'indisponibilità dell'infrastruttura ICT ha impatto bloccante su tutti i processi.

- Alta
  L'indisponibilità dell'infrastruttura ICT ha impatto sul processo di cura dei pazienti. Le prestazioni sanitarie non sono bloccate in quanto i dati relativi ai pazienti vengono registrati manualmente.

- Media
  L'indisponibilità dell'infrastruttura ICT è relativa ad attività non inerenti il processo di cura dei pazienti ma che possono avere un impatto su obblighi contabili e fiscali. Nell'intervallo di indisponibilità dell'infrastruttura ICT le attività, salvo la disponibilità delle commodities di base (elettricità ed accesso agli edifici), possono essere eseguite manualmente.

- Bassa
  L'indisponibilità dell'infrastruttura ICT è relativa ad attività di supporto che, anche se inattive per un certo periodo di tempo, non impattano sui servizi primari dell'azienda ospedaliera.

I livelli di Tier sono stati definiti coerentemente con le definizioni dell'Agid [2]

Livello Tier	**Principali Indicatori**			**Elementi di Massima della Soluzione Tecnica (minimo 2 siti)**	
	RTO		**RPO Max**	**Modalità minime di copia/aggiornamento per il conseguimento dei valori max. di RPO**	**Aspetti minimali connessi al sito di DR**
	Min.	Max.			
TIER 3	1 g	3 g	1 g	Electonic vaulting: soluzione che comporta il backup dei dati presso il sito alternativo in maniera elettronica, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time piu' veloce	Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile e con replica costante dei dati. Il backup avviene in modalità elettronica e quindi sono necessari collegamenti fra i siti tenuto conto della tipologia, quantità e periodicità dei dati da backup-are
TIER 4	4h	3gg	Max 4 h	Asincrono On line (risorsa storage accesa)	Il sito alternative è solitamente "un duplicato" del sito originale con tutti i sistemi hardware e la quasi totalità dei backup di dati disponibile. Il sito alternativo può essere pronto ed operativo in alcune ore o meno. Nel caso in cui il personale deve essere spostato fisicamente presso il sito secondario, il sito risulterà operativo solo dal punto di vista del data processing. La piena operatività sarà raggiunta quando anche il personale avrà raggiunto il sito
TIER 5	1h	Max. 4 h	Max. 5 min.	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi ciascuno con capacità sufficiente a prendere in carico il lavoro dell'altro e in cui l'aggiornamento del dato avviene solo quando entrambi i siti hanno completato l'update (con perdita dei soli i dati che in quel momento stanno per essere processati). E' fondamentale, per questa tipologia di

Livello Tier	Principali Indicatori			Elementi di Massima della Soluzione Tecnica (minimo 2 siti)	
	RTO		RPO Max	Modalità minime di copia/aggiornamento per il conseguimento dei valori max. di RPO	Aspetti minimali connessi al sito di DR
	Min.	Max.			
					soluzione, valutare la distanza fra i siti.
TIER 6	0m	1h	Zero min	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi, ognuno dei quali possiede capacità sufficienti a farsi carico del lavoro dell'altro; in questa soluzione il carico di lavoro da un sito all'altro si trasferisce immediatamente ed automaticamente. E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti

Si indica come RTO Recovery Time Objective, il tempo di ripristino del servizio ovvero la durata di tempo entro il quale un business process deve essere ripristinato dopo un disastro o una condizione di emergenza
Si indica come RPO Recovery Point Objective il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza [2].

I servizi erogati dall'AO Pini sono stati classificati a livello di tier e classe di criticità come riportato nella sottostante tabella.

Servizi	Livello di Tier	Classe di Criticità	Fornitore applicativo
Ambito Sanitario			
Pronto Soccorso	5	Alta	Engineering
Gestione Ricoveri	5	Alta	Engineering
Gestione Sale Operatorie	5	Alta	Dedalus
Anatomia Patalogica	5	Alta	Dedalus
Repository Referti Clinici	4	Media	Santer
Sistemi di Radiodiagnostica	5	Alta	Agfa
Laboratorio di analisi	4	Alta	Engineering
Gestione ambulatoriale	**5**	**Alta**	**Engineering**
Integrazione Cup Regionale	5	Media	Engineering
Cup	5	Alta	Engineering
Esposizione Referti su FSE	5	Media	Engineering
Gestione Amministrativa			
Gestione Amministrativa Contabile	5	Media	Engineering
Logistica e Supply Chain	5	Media	Engineering
Gestione Asset Aziendali	5	Media	Engineering
Gestione Risorse Umane	5	Media	Engineering
Gestione Delibere e Protocollo	4	Media	Engineering
Servizi trasversali			

Servizi	Livello di Tier	Classe di Criticità	Fornitore applicativo
Posta Elettronica	4	Media	Engineering
Portale Internet e Intranet	4	Media	Engineering

1.4.2 Variazioni eventuali nel numero dei servizi e relative criticità

n/a.

1.5 Matrice Servizi – Infrastrutture ICT – Presidi

La gestione dei sistemi informativi a supporto dei servizi in ambito sanitario ed amministrativo è esternalizzata e viene garantita tramite assistenza remota e/o presidio operativo nei giorni ed orari elencati nella tabella seguente.

Nelle fasce orarie di assenza del presidio, è prevista la reperibilità da parte dei fornitori.

Servizi	Sistemi ICT a supporto Interno/Fornitore	Fornitore	Localizzazione del presidio	Prestazione del Servizio
Ambito Sanitario				
Pronto Soccorso	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Prestazioni Ambulatoriali	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Ricoveri	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Sale Operatorie	Fornitore	Dedalus	Sede fornitore	Reperibilità h24 x 365 giorni
Anatomia Patalogica	Fornitore	Dedalus	Sede fornitore	Lun – Ven 07:30 – 13:00 e 14:00 – 17:00 (festivi esclusi)
Repository Referti Clinici per SISS	Fornitore	Santer	Sede fornitore	Reperibilità h24 x 365 giorni
Sistemi di Radiodiagnostica	Fornitore	Agfa	Sede fornitore	Personale TSRM - Amministratori di Sistema RIS-PACS dell'AO Pini per supporto applicativo di2° livello. Assistenza Tecnica di 3° livello, Telefonica e in Reperibilità h24 x 365 giorni da parte del fornitore
Conservazione Legale e Sostitutiva dei Referti Radiologici	Fornitore	Agfa	AO Pini Piazza A. Ferrari 1 Milano	
Laboratorio di analisi	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1	Presidio AO Pini Lun-Ven 8.00 – 17.00

Servizi	Sistemi ICT a supporto Interno/Fornitore	Fornitore	Localizzazione del presidio	Prestazione del Servizio
			Milano	Reperibilità h24 x 365 giorni
Trasfusionale	Sistemi in service Policlinico di Milano		Sede Policlinico	
Integrazione Cup Regionale	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Code Pazienti	Fornitore	Artexe	AO Pini Piazza A. Ferrari 1 Milano	Reperibilità h24 x 365 giorni
Ambito amministrativo contabile				
Gestione Amministrativa Contabile	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Logistica e Supply Chain	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Asset Aziendali	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Risorse Umane	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Gestione Delibere e Protocollo	Fornitore	Engineering	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 8.00 – 17.00 Reperibilità h24 x 365 giorni
Posta Elettronica	Fornitore/Gestore	NPO SISTEMI	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 7.30 – 17.00 Reperibilità h24 x 365 giorni
Portale Internet e Intranet	Fornitore/Gestore	NordCom	AO Pini Piazza A. Ferrari 1 Milano	Lun-Ven 8.00 – 17.00
Rete Dati e Network management	Fornitore/Gestore	Fastweb	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 7.30 – 17.30 Reperibilità h24 x 365 giorni
Rete di Fonia	Fornitore/Gestore	Fastweb	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 7.30 – 16.30 Reperibilità h24 x 365 giorni
System Management	Fornitore/Gestore	NPO SISTEMI	AO Pini Piazza A. Ferrari 1 Milano	Presidio AO Pini Lun-Ven 7.30 – 17.00 Reperibilità h24 x 365 giorni
Fleet Managemnet	Fornitore/Gestore	Nordcom	AO Pini Piazza A. Ferrari 1	Presidio AO Pini Lun-Ven 7.30 – 18.30

Servizi	Sistemi ICT a supporto Interno/Fornitore	Fornitore	Localizzazione del presidio	Prestazione del Servizio
			Milano	Reperibilità h24 x 365 giorni
Help Desk 1° livello	Fornitore	Nordcom	Sede NordCom	h24 x 365 giorni

2 Predisposizione all'emergenza ICT

E' stata definita una struttura organizzativa che, riportando e collaborando con il comitato di crisi dell'azienda ospedaliera, ha l'obiettivo di gestire le criticità e le emergenze in ambito ICT. L'organigramma della struttura organizzativa deputata per la continuità operativa, in cui vengono esplicitati i soggetti appartenenti alle singole componenti della struttura organizzativa per la continuità, è descritta nel piano di continuità operativa cui si rimanda per eventuale approfondimento.

2.1 La struttura organizzativa per la continuità ICT

La struttura organizzativa per la gestione della continuità operativa ICT dell'azienda ospedaliera G. Pini risulta così composta:

ORGANIZZAZIONE	RESPONSABILITÁ	RISORSE
Responsabile Continuità Operativa ICT	Gestione ordinaria: Responsabile della redazione del piano di continuità operativa ICT, della sua gestione e manutenzione; dell'adeguamento periodico del BIA (Business Impact Analysis), di studi e scenari finalizzati alla continuità operativa. Ha rapporti con i fornitori, le strutture tecniche, le assicurazioni e promuove attività di sensibilizzazione. Gestione straordinaria: • Valuta le situazioni di emergenza ICT • Coopera con il comitato di crisi dell'azienda ospedaliera per la gestione dell'emergenza • Dichiara lo stato di crisi ICT, gestisce i rapporti esterni e interni, attiva il processo di rientro. • Coordina le attività in fase di emergenza ICT	Responsabile dei Sistemi Informativi
Comitato di crisi ICT	Gestione ordinaria: Collabora al processo di continuità operativa ICT e contribuisce alla stesura del piano di continuità ICT; valuta periodicamente il livello di maturità della continuità operativa ICT e promuove il miglioramento continuo.	Responsabile dei Sistemi Informativi e collaboratori

ORGANIZZAZIONE	RESPONSABILITÁ	RISORSE
	Gestione straordinaria: • Attiva per la parte di sua competenza tutti i mezzi e risorse per la risoluzione del guasto • Collabora con il responsabile della continuità operativa ICT per predisporre il ritorno alla normalità	
Struttura Tecnica	Gestione ordinaria: Responsabile di tutte le attività operative e tecniche connesse con l'esecuzione delle procedure di recupero e rientro, ovvero esercitazioni e test periodici e manutenzione dell'infrastruttura tecnologica ed applicativa di recupero. Gestione straordinaria: • Attività per switching servizi ICT su sito alternativo • Ripristino dei server e delle infrastrutture • Restore dei Dati • Riallineamento dei dati • Verifica ritorno alla normalità	SIA Service manager dei fornitori per situazioni critiche inerenti sistemi di base, rete dati e fonia, applicativi di area clinica ed amminsitrativo contabile.

2.1.1 Comitato di crisi AO G.Pini

Il comitato di crisi dell'azienda ospedaliera G.Pini, con riferimento alle delibere 29/2013 e 243/2013, è stato così definito:

Funzione Aziendale	Persona	Telefono Orario di Lavoro	Telefono Reperibilità	Email
Direttore Amministrativo	Dott. Renato Malaguti	02.58296.200	.	direzionegenerale@gpini.it
Direttore Sanitario	Dott. Nunzio Buccino	02.58296.200	-	direzionegenerale@gpini.it
Responsabile del SIA	Ing. Francesca De Giorgi	02.58296.853	60071	segreteria.sia@gpini.it
Direttore UO Gestione Tecnico Patrimoniale	Ing. Massimiliano Agistri	02.58296.700	60082	Servizio.Tecnico.Pat@gpini.it
Direttore Medico di Presidio	Dott.ssa Paola Navone	02.58296.260	60164	direzione.medica@gpini.it

2.1.2 Responsabile della Continuità Operativa ICT

Funzione Aziendale	Persona	Telefono	Email
Responsabile dei Sistemi Informativi Aziendali	Ing. Francesca De Giorgi	02.58296.853	segreteria.sia@gpini.it

2.1.3 Comitato di Crisi ICT

Il comitato di crisi ICT, che collabora e riporta al comitato di crisi dell'azienda ospedaliera Gaetano Pini, è composto dal personale SIA con capacità decisionali, tecniche e organizzative per gestire l'emergenza e si avvale di una struttura tecnica composta dai referenti dei singoli fornitori (service manager) e dalle risorse di presidio per la gestione delle criticità relative ad applicativi ed infrastrutture, i quali sono tecnicamente responsabili delle attività operative e di recovery.

3 Business continuity

L'infrastruttura ICT dell' Azienda Ospedaliera garantisce un elevato livello di Business Continuity.
La rete dati e fonia è stata realizzata in modo che i collegamenti siano ridondati; in caso di indisponibilità di uno dei due link, la trasmissione dati è garantita dall'altro link.
Per la rete fonia sono stati previsti due centri stella, uno ubicato presso l'edificio "Principe" della sede centrale di piazza Cardinale Ferrari, l'altro presso la sede di via Isocrate. Nel centro stella della sede centrale (Piazza Cardinal Ferrari) sono state previste due centrali telefoniche ridondate.
Relativamente all'infrastruttura di sistema, sono state realizzate presso la sede centrale, piazza Cardinal Ferrari, due sale server ciascuna dotata di UPS adeguatamente dimensionati, collegate alla linea elettrica privilegiata e dislocate in locali separati (una presso la "Palazzina Officine", l'altra in corrispondenza della centrale termica). I server che ospitano i moduli applicativi ed i servizi di sistema sono replicati nelle due sale ed i moduli software di area clinica ed amministrativo contabile, oggetto di fornitura della società Engineering, sono in configurazione cluster active-active così che in caso di indisponibilità di una sala server, gli applicativi continuano a funzionare sui server del data center "secondario".
Gli applicativi di gestione del servizio di Radiodiagnostica sono anch'essi configurati in cluster, tuttavia richiedono intervento manuale sulle modalità diagnostiche (la cui gestione è in carico al servizio di Ingegneria clinica) da parte degli amministratori di sistema, al fine di dirottare il flusso di archiviazione delle immagini diagnostiche verso il sistema secondario, ubicato presso la sede di Via Isocrate.
La documentazione di riferimento è indicata nel par.3.10.

3.1 Ubicazione Data Center

L' Azienda Ospedaliera dispone di un sito primario e di un sito secondario/alternativo. I siti rispondono alla definizione introdotta dall'Agenzia per l'Italia Digitale di *Data Center Small*, ovvero locale con una superficie fino a 150 metri quadri, con sistema di controllo degli accessi tramite badge o codice pin, dotati di sistemi di alimentazione e di raffreddamento ridondati per garantire valori di temperatura e umidità costanti
La presenza di un data center primario ed uno alternativo, garantisce la continuità di servizio in caso di indisponibilità temporanea di una delle due sale e permette di fatto il recovery dei dati in caso di failure (disaster recovery) .

I dati logistici dei data center sono elencati nella tabella seguente :

Componente	Data Center Primario	Data Center Alternativo
Applicativi	AO PINI Palazzine Officine piano 1 Piazza A. Ferrari 1 – Milano	AO PINI Edificio Centrale Termica piano -2 Piazza A. Ferrari 1 – Milano
Servizi NOC – Dati	AO PINI Palazzine Officine Piazza A. Ferrari 1 - Milano	AO PINI Edificio Centrale Termica Piazza A. Ferrari 1 – Milano
Servizi NOC – Fonia	AO PINI Padiglione Principe pano -1 Piazza A. Ferrari 1 - Milano	AO PINI Via Isocrate 19 – Milano
RIS/PACS	AO PINI Monoblocco A piano rialzato Piazza A. Ferrari 1 - Milano	AO PINI Via Isocrate 19 – Milano

3.2 Infrastrutture di continuità e protezione fisica

L'azienda ospedaliera ha previsto sia collegamenti alla linea elettrica privilegiata che gruppi di continuità dedicati presso i siti primari e alternativi ed in ogni nodo di piano in modo da garantire, in caso di temporanea assenza di energia elettrica il funzionamento di server ed apparati.
Entrambi i data center sono dotati di sistemi di raffreddamento, antincendio, antifumo ed antiallagamento.
Per i dettagli tecnici degli impianti e dei locali dei data center si rimanda ai relativi progetti esecutivi, archiviati presso UOGTP.

Sito	Riferimenti Documenti di Progetto Esecutivo
AO PINI Palazzine Officine Piazza A. Ferrari 1 – Milano	Documenti disponibili c/o UOGTP
AO PINI Edificio Centrale Termica Piazza A. Ferrari 1 – Milano	Documenti disponibili c/o UOGTP
AO PINI Padiglione Principe Piazza A. Ferrari 1 – Milano	Documenti disponibili c/o UOGTP
AO PINI Via Isocrate 19 – Milano	Documenti disponibili c/o UOGTP

Per i servizi di gestione delle postazioni di lavoro, l'azienda ospedaliera G. Pini ha aderito alla gara regionale di Fleet Management. I software di supporto relativi al servizio sono gestiti dal provder Nordcom, direttamente presso i propri data center. I riferimenti alla soluzione di continuità del servizio adottati dal provider Nordcom sono descritti nel seguente documento :

Data Center Primario e Secondario di NordCom	RTI Costituendo NordCom/Dsc digital system computer srl "Allegato 2 Offerta Tecnica" per Gara 4/2011/LI - Procedura ristretta ai sensi del D.Lgs. 163/2006 per la selezione di operatori per i servizi di gestione delle postazioni di lavoro (fleet management) delle aziende sanitarie pubbliche di Regione Lombardia.

3.3 Controllo accessi ai data center

Per l'accesso ai siti dove sono collocati server e apparati, è stata fornita alla portineria di Via Pini 3 e di via Isocrate la lista del personale autorizzato ad accedere ai data center. In portineria, aperta h24 per 365 giorni all'anno, dopo la fase di riconoscimento del personale, vengono forniti gli strumenti elettronici di controllo accesso e le chiavi (necessarie per accedere ai locali in caso di mancanza di corrente elettrica) .

Sono state predisposte presso l'azienda ospedaliera i seguenti sistemi di controllo accessi :

Sito presso AO Pini	Controllo Accessi
Palazzine Officine Piazza A. Ferrari 1 – Milano	Badge RFID e Chiavi
Edificio Centrale Termica Piazza A. Ferrari 1 – Milano	Badge RFID e Chiavi
Padiglione Principe Piazza A. Ferrari 1 – Milano	Badge AO Pini e Chiavi
AO PINI Via Isocrate 19 – Milano	Badge AO Pini e Chiavi

I dettagli dei passi da seguire e degli strumenti da seguire per accedere ai locali sono definiti in

Componente	**Procedura**
Accesso ai locali infrastrutture ICT	"Procedura di Controllo Accessi" – AO G.Pini

3.4 Ambiente logistico per la continuità

Gli ambienti di ogni sito sono dotati di postazione di base costituita da:

- Impianto di fonia fisso
- Scrivania

Non è stata predisposta una postazione di lavoro specifica avanzata in quanto gli interventi nei data center prevedono di operare sulle console dei server e degli apparati, accessibili tramite Notebook dotato di software adeguato.

3.5 Hardware e Software per soluzione di continuità

Come descritto nei paragrafi precedenti, la soluzione di continuità si basa sulla presenza di un data center primario ed uno secondario sia per la componente applicativa che infrastrutturale. In caso di indisponibilità di uno dei due data center, l'operatività viene salvaguardata o ripristinata grazie alla presenza di servizi installati presso l'altro data center. L'infrastruttura di rete dati, gli apparati e le connessioni sono per la loro stessa progettazione ridondati nei due nodi di core, così da permettere la continuità operativa. Per la fonia Voice Over Ip si ha comunque continuità in caso di caduta di un link all'interno di ciascuna delle due sedi dell'AO G.Pini.

Le applicazioni software a supporto dei servizi ospedalieri erogati, che sono state individuate quali oggetto di Disaster Recover , si suddividono in tre macro categorie: applicazioni in cluster, applicazioni ridondate e non ridondate. Le applicazioni in cluster sono rappresentate da tutte le applicazioni che, in caso di indisponibilità di un sito, garantiscono che il servizio continui a funzionare in modo trasparente per l'utente in quanto tutta l'elaborazione viene effettuata dal sito alternativo. Per le applicazioni ridondate ed installate in entrambi i siti, ma non in cluster, in caso di indisponibilità, il servizio può riprendere a funzionare sul sito alternativo solo dopo uno specifico intervento tecnico. Infine le applicazioni non ridondate, ovvero quelle installate solo in un sito, in caso di indisponibilità dello stesso non saranno fruibili fino al ripristino del relativo server.

I dettagli delle specifiche applicazioni sono riportati nella sottostante tabella :

	Cluster	Ridondate	Non Ridondate	Fornitore/Gestore
Pronto Soccorso	x			Engineering
Prestazioni Ambulatoriali	x			Engineering
Gestione Ricoveri Dipartimentali	x			Engineering
Integrazione Cup Regionale	x			Engineering
Esposizione Referti su FSE	x			Engineering
Laboratorio Analisi	x			Engineering
Gestione Amministrativa Contabile	x			Engineering
Logistica e Supply Chain	x			Engineering
Gestione Asset Aziendali	x			Engineering
Gestione Risorse Umane	x			Engineering
Gestione Delibere e Protocollo		x		Engineering
Portale Intranet e Internet			x	Engineering
Piattaforma di Integrazione Regionale			x	Santer
Gestione Sale Operatorie	x			Dedalus
Anatomia Patalogica	x			Dedalus

	Cluster	Ridondate	Non Ridondate	Fornitore/Gestore
Sistemi di Radiodiagnostica		x		Agfa
Conservazione Legale e Sostitutiva diimmagini radiologiche		x		Agfa
Firewall	x			Npo Sistemi
Proxy	x			Npo Sistemi
Posta Elettronica			x	Npo Sistemi
Sistema di Trouble Ticketing	X			NordCom

Relativamente alla connessione dati tra le sedi di via Isocrate e Piazza Cardinal Ferrari, che permette agli utenti di accedere agli applicativi, è previsto un collegamento punto a punto a 100 Mbit, Ad oggi per ognuna delle due sedi dell'AO Pini è installato un singolo router di accesso alla rete esterna ed alla rete Internet. In caso di fermo o guasto del router non si ha accesso ad Internet ed alla rete extranet SISS. La documentazione di riferimento è indicata nel par.3.10.

3.6 Back Up dei Dati Aziendali e restore

L'azienda ospedaliera si è dotata di un sistema di backup basato sul software IBM Tivoli che gestisce due tape library IBMTS3200, una per data center, con capienza per ciascuna libreria di 48 nastri LTO 4 corrispondenti a 800 Gb non compressi. Le due librerie sono collegate attraverso un canale in fibre channel. I dati aziendali e gli applicativi utilizzano i sistemi di storage condiviso e sono soggetti a policies di back up, almeno giornaliero, che permette la salvaguardia e il ripristino delle informazioni in caso di indisponibilità di una sala server e/o di alcuni server.
I criteri e le politiche di back up in essere presso l'AO sono riportati nella seguente procedura

Componente di Continuità	Procedura
Back Up	"Procedura di Gestione dei back Up" – AO G.Pini

La documentazione tecnica di riferimento è indicata nel par.3.10.

3.7 Interrelazioni dei sistemi ICT con altri sistemi esterni all'Azienda Ospedaliera

Alcuni sistemi a supporto dei servizi dell'AO PINI prevedono interrelazioni con sistemi IT esterni all'azienda ospedaliera ed in caso di malfunzionamento e/o arresto degli stessi, deve essere effettuata la verifica di invio e ricezione dei dati verso tali sistemi. I servizi dell'AO Pini che si interfacciano con sistemi esterni sono riportati nella sottostante tabella:

Servizi	**Sistemi Esterni**
Ambito Sanitario	
Pronto Soccorso	SISS • Pubblicazione link Referti sui domini centrali SISS tramite Repository INPS INPS AREU • Comunicazione Infortuni Inail
Prestazioni Ambulatoriali	SISS • Pubblicazione link Referti sui domini centrali SISS tramite Repository
Gestione Ricoveri	SISS • Pubblicazione link Lettere di dimissione sui domini centrali SISS tramite Repository INPS • Comunicazione inizio Ricovero per certificato malattia Inps
Gestione Trasfusionale	Integrazione vs SIMT Policlinico
Gestione Sale Operatorie	n/a
Anatomia Patalogica	n/a
Sistemi di Radiodiagnostica	SISS Pubblicazione link Referti sui domini centrali SISS tramite Repository
Laboratorio di	SISS Pubblicazione link Referti sui domini centrali SISS tramite Repository
Repository	SISS Archiviazione e notifica link Referti al SISS
Prestazioni Ambulatoriali	
CUP	Integrazione con CCR (Call Center Regionale)
Gestione Code Pazienti	n/a
Gestione Amministrativa AO Pini	
Gestione Amministrativa Contabile	Hub di Regione Lombardia • Invio e ricezione fatture attive e passive
Logistica e Supply Chain	n/a
Gestione Asset e Cespiti Aziendali	n/a
Gestione Risorse Umane	INAIL • Comunicazione Infortuni Inail INPS • Comunicazioni malattie dipendenti vs Inps
Gestione Delibere e Protocollo	n/a
Conservazione Legale e Sostitutiva	n/a
Posta Elettronica	n/a

Servizi	Sistemi Esterni
Servizi di infrastruttura	
Portale Internet e Intranet	n/a
Rete Dati	Accesso VPN da parte dei Fornitori
Rete di Fonia	Call center del servizio Fleet management regionale
Server e Network Management	n/a
Fleet Management e Help Desk	n/a

3.8 Infrastruttura di Rete interna

L'infrastruttura di rete segue il modello gerarchico a tre livelli e doppio centro stella, ovvero vi sono:

- Nodo di Core (CD)
- Nodi di Distribuzione (BD)
- Nodi di Piano\Accesso (FD)

Il doppio centro stella prevede l'interconnessione tra i due nodi di core tramite due cavi in fibra ottica monomodale garantendo la ridodanza nel caso di guasto di uno dei due cavi.
Analogamente i nodi di piano di piazza C.Ferrari sono connessi, sempre tramite cavi ridondati, ai nodi di distribuzione. Per la sede di via Isocrate, considerato che il numero ridotto di piani non giustifica una struttura a tre livelli, è presente un solo nodo con funzioni sia di distribuzione che di core collegato ai nodi di piano. Inoltre la sede di via Isocrate è connessa all'infrastruttura di rete ed ai server situati in piazza C. Ferrari.

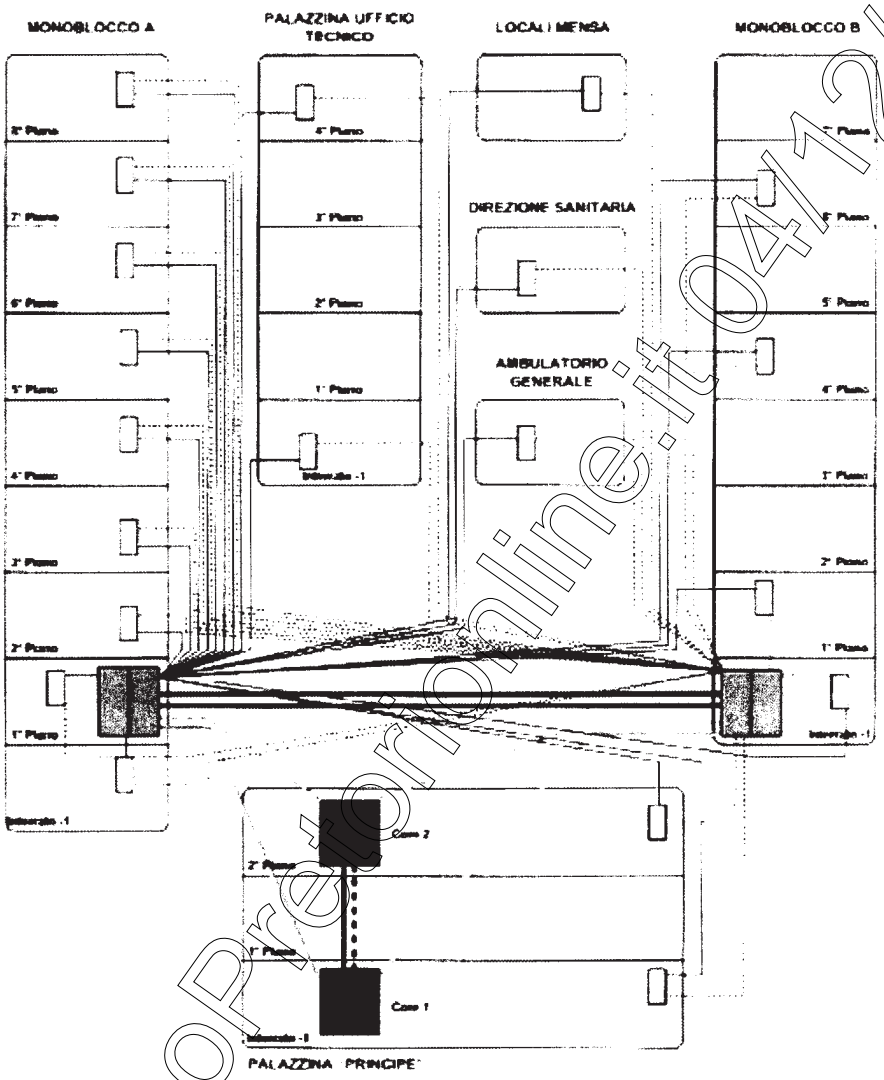

Fig. 1 Schema della rete dell'AO G .Pini per P. Cardinal Ferrari

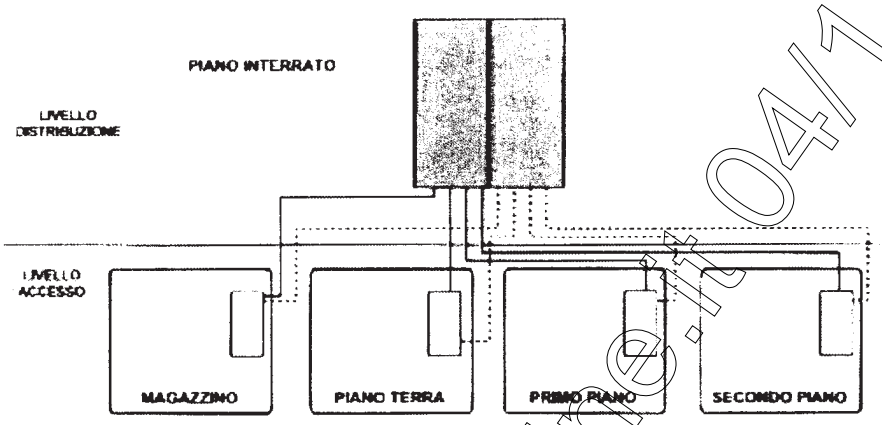

Fig. 2 Schema Rete di via Isocrate

I riferimenti ai dettagli dell'infrastruttura di rete dell'AO Pini sono elencati nel paragrafo **Errore. L'origine riferimento non è stata trovata.**

3.9 Gestione dei sistemi Hardware, Software e di rete in situazione di normalità

In condizioni di normalità i componenti hardware, software e di rete sono oggetto continuo di monitoraggio da parte del NOC. Il presidio sistemistico utilizza sistemi di monitoraggio (Nagios) con i quali è in grado di rilevare eventuali anomalie o fault sui componenti hardware, software e di rete. In caso di failure o fault di una componente di infrastruttura, il sistema Nagios segnala la situazione al presidio tecnico. I riferimenti ai documenti inerenti le soluzioni tecniche per il monitoraggio delle infrastrutture sono elencate nel paragrafo 3.10.

3.10 Documentazione

Tutte le informazioni di dettaglio relative alla configurazione dei sistemi sono riportate nei seguenti documenti:

Componente	Fornitore	Riferimento Documentale
Applicativi	Engineering	Offerta Tecnica di Engineering relativa all'Appalto per la Progettazione, Realizzazione, Manutenzione ed Evoluzione del sistema informatico aziendale dell'AO PINI di Giugno 2009 – Doc.3 Progetto Applicativo
Rete Dati	Engineering	Offerta Tecnica di Engineering relativa all'Appalto per la Progettazione, Realizzazione, Manutenzione ed Evoluzione del sistema informatico aziendale dell'AO PINI di Giugno 2009 – Doc..4 Progetto TecnologicoOfferta Tecnica di Engineering relativa all'Appalto per la Progettazione, Realizzazione, Manutenzione ed Evoluzione del sistema informatico

Componente	Fornitore	Riferimento Documentale
		aziendale dell'AO PINI di Giugno 2009 – Variante Cap.4 Progetto Tecnologico
Rete Fonia	Fastweb	Fornitura di servizi di gestione Infrastrutture fonia-dati NOC - Allegato 2 - Allegato tecnico Istituto Ortopedico Gaetano Pini
Storage	Engineering	Offerta Tecnica di Engineering relativa all'Appalto per la Progettazione, Realizzazione, Manutenzione ed Evoluzione del sistema informatico aziendale dell'AO PINI di Giugno 2009 – Doc.4 Progetto Tecnologico
Ris/Pacs	Agfa	Agfa Healthcare – Relazione di Progetto - Versione 1.4 del 12/03/2012
System Management	Npo Sistemi	NPO, Fastweb e Italtel – Documentazione tecnica di Procedura aperta aggregata del servizio di gestione delle infrastrutture di telecomunicazioni Network Operation Center (NOC)

4 Gestione dell'emergenza ICT e Disaster Recovery

4.1 Scenari di emergenza applicabili

I macro scenari che possono implicare situazioni di criticità sulle apparecchiature e infrastrutture IT e possono determinare una parziale o completa emergenza ICT sono stati categorizzati come riassunto in tabella:

Scenario	Cause
Indisponibilità delle *commodities* di base	○ Indisponibilità dell'elettricità ○ Temperature Elevate in Server Farm ○ Blocco/guasto dei server che ospitano servizi di base
Indisponibilità rete dati/fonia	○ Guasto apparati Centro Stella, nodi di distribuzione, nodi di accesso
Indisponibilità Applicativi	○ Anomalie Software ○ Attacchi informatici ○ Blocco/guasto dei server applicativi
Attacchi Informatici	○ Attacchi Dos ○ Implementazione di codice malevolo ○ Virus ○ Trojan

4.2 Fase di reazione all'emergenza

Con riferimento al Piano di Continuità Operativa, In fase di rilevazione di una situazione che si presenta come emergenza ICT, il responsabile della continuità operativa ICT, riportando al comitato di crisi dell'azienda ospedaliera, si adopera conformemente alle procedure aziendali per

- Dichiarare lo stato di emergenza ed attivare il comitato di crisi
- Notificare lo stato di emergenza alle strutture operative
- Gestione dell'emergenza
- Riattivazione dei servizi
- Ritorno alla normalità e relativa comunicazione

4.3 Dichiarazione e Notifica dell'emergenza ICT

Una volta rilevato che l'incident non è un una situazione di semplice anomalie o errore, ma un emergenza ICT, il responsabile della continuità operativa ICT si adopera per informare il comitato di crisi aziendale, a coordinare e convocare il comitato di crisi ICT e ad informare le strutture opportune per la risoluzione dell'emergenza, come descritto nel piano di continuità operativa, cui si rimanda per ogni approfondimento.

4.4 Fase di Gestione dell'emergenza

I macro scenari di crisi hanno come denominatore comune eventi tali che un sito sia parzialmente o completamente inattivo, per i quali si rende pertanto necessaria l'applicazione della procedura di emergenza ICT che prevede:

- La verifica del corretto funzionamento dei servizi ICT per le infrastrutture ed i server in cluster
- L'attivazione del personale tecnico, eventualmente ingaggiando i reperibili, per configurare il server/apparato alternativo in caso di sistema ridondato in modo da continuare o riprendere ad erogare il servizio
- L'innesco del personale tecnico, se necessario dei reperibili, addetti a quei server/apparati ed infrastrutture attualmente non ridondati.

4.5 Riattivazione dei Servizi e Ritorno alla Normalità

La fase di riattivazione dei servizi prevede la parziale o totale riaccensione delle infrastrutture di un sito, una fase di verifica di completamento a buon fine delle operazioni di riaccensione ed in ultimo la fase di allineamento dei dati. Quest'ultima operazione può, a secondo della tipologia di emergenze, comprendere il restore dei dati.
La sequenza di riaccensione dei server e apparati, insieme alle check list di verifica della riattivazione dei servizi, per ognuno dei data center aziendali, così come le operazioni di retore dei dati sono state definite nella seguenti procedure, cui si rimanda per ogni approfondimento:

Componente di Continuità	Procedura
Sala Server	"Procedura di Spegnimento e Accensione Sala CED A e Sala CED B" – AO G.Pini
Sala Apparati via Isocrate	"Procedura di Spegnimento e Accensione Apparati di via Isocrate" – AO G.Pini
Centro Stella	"Procedura di Spegnimento e Accensione *Vecchio* Centro Stella" – AO G.Pini
Restore dei Dati	"Procedura di Restore dei Dati" – AO G.Pini

4.6 Checklist per verifica rientro alla normalità

Una volta ripristinati i sistemi e l'infrastruttura che ne hanno determinato la situazione di emergenza, è necessario completare una checklist per certificare il rientro alla normalità.

CHECKLIST PER VERIFICARE L'EFFICIENZA DELLE AZIONI DI RIENTRO	ESEGUITO
Ripristino del supporto all'infrastruttura.	☐
Notifica alle altre amministrazioni ed entità esterne che possono essere impattate del ritorno della disponibilità dei servizi	☐
Installazione di hardware, software, firmware ove necessario	☐
Ripristino della connettività e delle interfacce con gli apparati di rete e con i sistemi esterni	☐
Test/verifica della piena funzionalità del sistema	☐
Modalità per il restore dei dati a partire dai backup	☐
Inserimento nei sistemi informatici dei dati eventualmente prodotti in formato cartaceo	☐
Rientro del personale alla normale operatività	☐

Nel caso di compilazione positiva di tutta la checklist, ovvero in caso siano state eseguite con esito positivo tutte le attività per il rientro alla normalità, viene dichiarato dal responsabile della continuità operativa ICT il rientro alla normalità e ne viene data tempestiva comunicazione al comitato di crisi ICT ed aziendale.

5 Formazione

Il piano di Formazione delle risorse per la continuità ICT e il Disaster Recovery prevede una sessione annuale, nella quale

- I componenti del comitato di crisi ICT vengono informati sulle procedure ed i loro aggiornamenti da seguire in caso di emergenza ICT
- Le strutture tecniche ICT rivedano e riesaminano le procedure per l'attivazione del sito alternativo e del restore dei dati

6 Gestione ed Aggiornamento del piano di Continuità Operativa

Il piano di Disaster Recovery, così come il piano di Continuità Operativa, è soggetto a revisione ed adeguamento a fronte di modifiche che vengono avvenire nell'organizzazione, nei contratti di fornitura e modifiche alle infrastrutture e al software. I dettagli sono descritti nel par. 6.2.

6.1 Modalità di Esecuzione dei Test Periodici

Verrà prevista per l'anno 2016 una fase di test con l'obiettivo di

- Verificare il corretto spegnimento e riaccensione di apparati e server.
- Controllare che in caso di indisponibilità di uno dei data center le applicazioni in cluster continuino ad erogare il servizio.
- Verificare che le applicazioni ridondate, in seguito ad intervento dei tecnici per le attività di start up dei server secondario, eroghino il servizio
- Controllare la correttezza del meccanismo del restore dei dati con applicazioni a campione

Le prove verranno realizzate in ambiente di test in modo da non interferire con l'operatività quotidiana

6.2 Modalità di Revisione e Adeguamento del Piano

Il piano di Continuità Operativa sarà oggetto di revisione, in caso di modifiche organizzativi, tecniche e contrattuali che possano impattare la continuità operativa ICT ovvero in caso di:

- Variazioni alla struttura organizzativa dell'azienda ospedaliera e del comitato di crisi della continuità operativa ICT
- Modifiche inerenti i fornitori di servizi ICT
- Introduzione o eliminazione di applicazioni software
- Variazione di criticità delle applicazione software
- Modifiche all'infrastruttura di rete
- Variazioni contrattuali per la reperibilità del personale tecnico
- Modifica della logistica in particolare inerenti i locali di sito primario e alternativo
- Stipula di nuovi contratti o cessazioni degli esistenti