IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

DELIBERAZIONE N. **486** DEL **23/04/2021**

OGGETTO: Approvazione il Piano per la transizione digitale dei servizi amministrativi e sanitari degli IFO per il triennio 2021 - 2023

Esercizi/o 2021/2023 Centri/o di costo . **- Importo presente Atto: € .** **- Importo esercizio corrente: € .** Budget **- Assegnato: € .** **- Utilizzato: € .** **- Residuo: € .** **Autorizzazione n°: .** Servizio Risorse Economiche: **Giovanna Evangelista**	STRUTTURA PROPONENTE **UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici** Il Dirigente Responsabile **Giuseppe Navanteri** Responsabile del Procedimento **Giuseppe Navanteri** L'Estensore **Anna Cirulli** Proposta n° DL-500-2021
PARERE DEL DIRETTORE SANITARIO Positivo Data 23/04/2021 IL DIRETTORE SANITARIO **Branka Vujovic**	**PARERE DEL DIRETTORE AMMINISTRATIVO** Positivo Data 22/04/2021 IL DIRETTORE AMMINISTRATIVO **Laura Figorilli**

Parere del Direttore Scientifico IRE **Gennaro Ciliberto** data 22/04/2021 Positivo

Parere del Direttore Scientifico ISG **Aldo Morrone** data 22/04/2021 Positivo

La presente deliberazione si compone di n° 7 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
- Allegato 1 composto da n. 45 pagine

Visto il decreto legislativo 30 dicembre 1992, n. 502 e successive modificazioni ed integrazioni;
il decreto legislativo 16 ottobre 2003, n. 288;

Vista la legge regionale 23 gennaio 2006, n. 2;

Visto il decreto legislativo 7 marzo 2005, n. 82/2005 e s.m.i.
l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 e approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019, modificato e integrato con Deliberazione n. 1254 del 2.12.2020, n. 46 del 21/01/2021 e n. 380 del 25.03.2021, approvate dalla Direzione Salute e Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30.03.02021

Premesso che l'art. 17 del D.Lgs. 7.3.2005 n. 82 - Codice dell'Amministrazione Digitale (aggiornato con le modifiche e integrazioni introdotte dal Decreto Legislativo n. 217 del 13.12.2017), rubricato "Responsabile per la transizione al digitale e difensore Civico", stabilisce che ciascuna amministrazione sia tenuta ad affidare ad un unico ufficio dirigenziale, fermo restando il numero complessivo degli uffici, la "*transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità", n*ominando un Responsabile per la Transizione al Digitale (RTD).

Atteso che il citato art. 17 attribuisce al Responsabile per la transizione al digitale compiti di coordinamento e di impulso ai processi di reingegnerizzazione dei servizi, quali in particolare:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazioni e fonia;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;

d) accesso dei soggetti disabili agli strumenti informatici e promozione della accessibilità;

e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché' di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione;

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno della amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, nonché delle norme in materia di accessibilità e fruibilità.

Vista la Circolare n. 3 del 1° Ottobre 2018 del Ministro della Pubblica Amministrazione la quale invita tutte le amministrazioni ad individuare al loro interno un Ufficio per la Transizione al Digitale e un Responsabile quale figura di riferimento e punto di contatto con l'Agenzia per l'Italia Digitale e la Presidenza del Consiglio dei Ministri, per le questioni connesse alla trasformazione digitale delle Pubbliche Amministrazioni, nonché per la partecipazione a consultazioni e censimenti previsti

Rilevato che al fine di garantire la piena operatività dell'Ufficio per la Transizione al Digitale la citata Circolare n. 3/2018 prevede per il Responsabile, oltre ai compiti espressamente previsti dall'art. 17 del CAD, anche quelli sotto indicati in ragione della trasversalità della funzione:

a) il potere del RTD di costituire tavoli di coordinamento con gli altri dirigenti della amministrazione e/o referenti nominati da questi ultimi;

b) il potere del RTD di costituire gruppi tematici per singole attività e/o adempimenti (ad esempio: pagamenti informatici, piena implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.);

c) il potere del RTD di proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT);

d) l'adozione dei più opportuni strumenti di raccordo e consultazione del RTD con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali);

e) la competenza del RTD in materia di predisposizione del Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale;

f) la predisposizione di una relazione annuale sull'attività svolta dall'Ufficio da trasmettere al vertice politico o amministrativo che ha nominato il RTD".

Considerato che con Deliberazione n. 185 del 16 febbraio 2021 si è individuata l'UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici quale Ufficio referente per la transizione digitale degli IFO e, contestualmente, si è nominato l'ing. Giuseppe Navanteri, Responsabile della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici, come Responsabile per la transizione al digitale;

che gli IFO hanno predisposto un documento programmatico valido per il triennio 2018-2020 e inerente l'attività informatica sanitaria ed amministrativa, approvato con Determinazione n. 1019 del 7 dicembre 2017

Valutati i compiti di indirizzo, di pianificazione e di coordinamento attribuiti al Responsabile per la transizione al Digitale dalla norma e riportati nella Determinazione di nomina

Rilevata la necessità di aggiornare il citato documento programmatico con le risultanze dell'analisi dei fabbisogni hardware/software nel frattempo condotta e della disamina dell'asset tecnologico e applicativo in uso ed operanti in IFO

Considerato che a tali studi è seguita, di concerto con la Direzione IFO, l'attività pianificazione:

- degli interventi di manutenzione adeguativa/evolutiva del software
- di acquisizione di nuovi software/servizi applicativi
- di upgrade dell'hardware in uso
- di fornitura di nuove apparecchiature

che il documento finale così predisposto assume la funzione di strumento strategico e di pianificazione del processo di digitalizzazione per il triennio 2021-2023, con l'obiettivo di guidare e fornire supporto alla trasformazione digitale dei servizi sanitari ed amministrativi degli IFO, anche alla luce delle criticità determinate dalla Pandemia da Covid-19 e delle indicazioni fornite dall'Agenzia per l'Italia Digitale (AgID) e dal Dipartimento per la Trasformazione digitale

Valutata positivamente l'opportunità di intitolare il documento come "*Piano per la transizione digitale dei servizi amministrativi e sanitari per il triennio 2021-2023*" per tener conto degli obiettivi e delle finalità del documento medesimo

Considerato che i finanziamenti previsti per l'attuazione degli interventi di investimento previsti dal documento sono di provenienza Ministeriale e/o Regionale

Rilevato che il presente provvedimento non comporta oneri a carico dell'Ente

Attestato altresì che il Dirigente proponente il presente provvedimento, sottoscrivendolo attesta, in particolare, che lo stesso è predisposto nel pieno rispetto delle indicazioni e dei vincoli stabiliti dai decreti del Commissario ad acta per la realizzazione del Piano di Rientro dal disavanzo del settore sanitario della Regione Lazio;

PROPONE

Per i motivi di cui in narrativa che si intendono integralmente confermati di approvare il *Piano per la transizione digitale dei servizi amministrativi e sanitari per il triennio 2021-2023* di cui all'allegato 1 alla presente deliberazione.

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

Il Direttore Generale

Visto	il decreto legislativo 30.12.1992, n. 502 e successive modificazioni ed integrazioni;
Vista	la legge regionale 23.01.2006, n. 2;
Visto	l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019;
In virtù	dei poteri conferitigli con decreto del Presidente della Regione Lazio n. T00248 del 23.11.2016.
Preso atto	che il Dirigente proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e s.m., nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.
Visto	il parere favorevole del Direttore Amministrativo e del Direttore Sanitario Aziendale;

ritenuto di dover procedere;

Delibera

di approvare la proposta così formulata concernente *"Approvazione il Piano per la transizione digitale dei servizi amministrativi e sanitari degli IFO per il triennio 2021 - 2023"* e di renderla disposta.

Il Direttore Generale
Dott. Francesco Ripa di Meana
Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

SISTEMA SANITARIO REGIONALE
IRCCS
ISTITUTI FISIOTERAPICI
OSPITALIERI

IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA
ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Piano per la transizione digitale dei servizi amministrativi e sanitari per il triennio 2021-2023

Il Responsabile della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici e RTD: **Ing. Giuseppe Navanteri**

Il Direttore Generale: **Dott. Francesco Ripa di Meana** _____

Il Direttore Sanitario Aziendale: **Dott.ssa Branka Vujovic** _____

Il Direttore Amministrativo: **Dott.ssa Laura Figorilli** _____

Sommario

Contesto di riferimento

L'Organizzazione Mondiale della Sanità (OMS) ha, di recente, pubblicato l'esito di uno studio del 2018[1], dal quale emergono le raccomandazioni per utilizzare al meglio le tecnologie dell'innovazione nel campo della sanità digitale. Il documento è un'importante testimonianza delle opportunità offerte dalla tecnologia per migliorare i livelli di assistenza sanitaria sul territorio, in particolare lo studio approfondisce i benefici per supportare il management aziendale nelle fasi di decision-making, per ottimizzare la gestione dei farmaci, per migliorare il rapporto con il paziente e per promuovere la Telemedicina.

Partendo dal documento dell'OMS e da altri studi e ricerche disponibili in letteratura, gli IFO, in relazione anche allo stato di attuale di utilizzo delle tecnologie, hanno adottato un piano costante e di graduale miglioramento dei servizi che ricomprende l'aggiornamento dei dispositivi di ausilio all'attività sanitaria e l'implementazione di nuovi processi secondo gli approcci della *Mobile Health* e del *Full digital*.

Il Piano Triennale degli IFO è stato predisposto, peraltro, basandosi sul precedente Piano Triennale da un punto di vista della sicurezza del dato (GDPR n. 679/2016) e della digitalizzaizone del percorso clinico assistenziale ma anche in accordo al quadro normativo vigente, in particolare con riferimento al Piano Triennale per l'informatica nella Pubblica Amministrazione 2019-2021 e alle linee guida emanate dall' Agenzia per l'Italia Digitale nell'ultimo biennio, con uno sguardo all'innovazione. Al riguardo, pare opportuno dare risalto al progetto sperimentale del Dipartimento della Funzione Pubblica (di seguito DFP) che, a seguito dell'emanazione delle Linee guida n. 1/2017 e n. 2/2017 e ai sensi di quanto previsto dall'art. 8 del d.lgs 150 del 2009, sta perseguendo l'obiettivo di identificare un set di indicatori di performance (che riporterà indicatori in parte comuni e in parte specifici in relazione alle particolari specifità delle PA) a cui le amministrazioni centrali e territoriali dovranno obbligatoriamente far riferimento. Tale progetto prevede, in sintesi, l'inserimento di Key Performance Indicator (KPI) per varie dimensioni di analisi: per il settore IT, in particolare, il DFP prevede l'inserimento di indicatori direttamente correlati alle linee di azione del Piano Triennale per l'informatica nella Pubblica Amministrazione ed individuati di concerto con l'Agenzia per l'Italia Digitale. In tale prospettiva è di conseguenza necessario l'allineamento dei vari documenti strategici emanati dagli IFO. Può, al riguardo, essere utile definire un albero della performance come mappa logica che rappresenti graficamente i legami tra la missione, le aree strategiche, gli obiettivi strategici, le iniziative progettuali di supporto e i relativi indicatori di outcome.

E' in pratica la rappresentazione di come gli obiettivi di diversa natura possano fornire contributi all'interno di un disegno strategico complessivo coerente. Per quanto esposto, è evidente che il Piano rappresenti uno strumento in continua evoluzione, che va nella direzione di un utilizzo sempre più esteso delle tecnologie e delle innovazioni al fine di assicurare un servizio sanitario sempre più efficace ed efficiente.

[1] cfr. https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/

Linee guida per il Piano Triennale per l'informatica nella Pubblica Amministrazione

Il nuovo Piano Triennale per l'informatica nella Pubblica Amministrazione, predisposto dall' Agenzia per l'Italia Digitale (di seguito *AgID*) ed emanato con Decreto del Ministro della Pubblica Amministrazione, delinea gli indirizzi per attuare la strategia di digitalizzazione e di innovazione tecnologica del Paese.

Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito *Piano AgID* per distinguerlo con il Piano Triennale IFO) si pone in continuità con le versioni precedenti e con il Modello strategico già individuato adeguando le linee di azione ivi riportate alle mutate condizioni dello scenario normativo e tecnologico.

Sono riaffermati, di conseguenza, i principi base che recepiscono le linee di evoluzione già affermate con l'Agenda digitale europea che costituisce una delle sette iniziative faro della strategia "Europa 2020":

- Digital per default
- Cloud first
- Once only
- Speed only

Tutte le amministrazioni, comprese le aziende ospedaliere, sono tenute pertanto ad adeguare i propri piano di sviluppo ai principi su menzionati e a recepire le linee di indirizzo dettate dal Piano AgID.

Il principio "Digital per default" è il principio guida, esprimendo il concetto che ogni nuovo processo deve essere digitalizzato ("Full digital") e che, di conseguenza, ogni Amministrazione deve porre in essere gli interventi, anche graduali, necessari a digitalizzare tutti i processi di competenza.

La digitalizzazione deve peraltro essere condotta individuando soluzioni architetturali che prevedano, in prima analisi, il ricorso a piattaforme Cloud ("Cloud first"), utilizzando i dati già disponibili in altre amministrazioni ("Once only") e ricorrendo alla piattaforma Speed per l'autenticazione degli utenti ("Speed only").

In accordo ai su esposti principi, il Piano AgID:

- recepisce le ultime modifiche al Codice dell'Amministrazione Digitale (CAD)
- rafforza il paradigma Cloud della PA;
- introduce nuovi modelli e strumenti per l'innovazione per la PA e in particolare riferimento ai temi dell'open innovation e al paradigma smart landscape;
- sensibilizza le amministrazioni sui temi delle competenze manageriali e digitali.

Linee guida AgID

AgID adotta le seguenti tipologie di linee guida ai sensi degli articoli 14-bis e 71 del CAD, o di specifiche disposizioni normative:

- di indirizzo che rimandano per gli aspetti di dettaglio alle disposizioni da emanare a cura della singola Amministrazione
- regole tecniche
- operative

L'efficacia delle linee guida è a partire dal giorno successivo a quello della loro pubblicazione sul sito istituzionale di AgID, ai sensi dall'articolo 71 del CAD.

Nel presente documento si fa riferimento, esplicitamente o implicitamente, alle seguenti linee guida:

- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate v.1.1
- Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni
- Linee guida Indice PA
- Linee guida di design per i servizi digitali della PA
- Guida pratica per la creazione di un documento accessibile
- Modello di rapporto conclusivo di accessibilità
- Linee Guida per il Disaster Recovery (DR) delle PA
- Linee guida per la marcatura dei documenti normativi secondo gli standard normeinrete
- Caratterizzazione dei sistemi cloud per la pubblica amministrazione
- Linee Guida della razionalizzazione per l'infrastruttura digitale nella Pubblica Amministrazione
- Linee guida per il contrassegno generato elettronicamente
- Linee guida per la presentazione dei piani di progetto regionali per il Fascicolo Sanitario Elettronico

Struttura del Piano per la transizione digitale

l Piano è distinto in due sezioni, la prima ("Digitalizzazione e Innovazione tecnologica") è relativa alla descrizione delle linee di azione e degli interventi di carattere "trasversale" che riguardano sia le strutture amministrative sia quelle sanitarie nonché le attività e gli interventi di supporto alla ricerca.

La seconda sezione descrive gli interventi che riguardano la struttura sanitaria e l'attività di ricerca che, utilizzando il termine che AgID ha coniato per identificare l'ecosistema corrispondente, si indicherà come Sanità digitale.

La sezione **I** "Digitalizzazione e Innovazione tecnologica" ricomprende i seguenti interventi:

- Sicurezza informatica
- Protezione dei dati
- Gestione documentale e conservazione digitale
- Comunicazione istituzionale
- Digitalizzazione dei processi interni e di back office
- Potenziamento infrastrutturale

La sezione **II** "Sanità digitale" ricomprende:

- Cartella clinica elettronica (cce) di reparto ed ambulatoriale
- PDTA – Data warehouse – Business Intelligence
- Processo digitalizzato di consenso informato e consenso al trattamento dei dati sensibili
- Digitalizzazione del processo chirurgico ivi compresa la preospedalizzazione
- Prescrizione/ricette dematerializzate
- Sistema digitale ed interattivo con il paziente per la prenotazione esami medico nucleare
- Sistema di cartella clinica e gestione percorso paziente per i trattamenti radioterapici
- Realizzazione di un nuovo sistema di gestione dell'anatomia patologica ed integrazione dello stesso al percorso clinico assistenziale digitale
- Progetto paperless per eliminazione dei documenti sanitari cartacei digitalizzati su conservazione sostitutiva
- Potenziamento infrastruttura hardware funzionale al percorso sanitario (rete wi-fi, potenziamento segnale mobile voce e dati all'interno della struttura ifo, bonifica infrastruttura di rete e armadi rack, potenziamento blade già operativo e acquisto nuovo server blade)
- Disaster recovery in cloud
- Semplificazione della procedura di richiesta di invalidità civile - inps

La sezione **III** "Piano investimenti Ingegneria Clinica e Tecnologie e Sistemi Informatici 2021 - 2023" ricomprende le schede dei costi.

SEZIONE I:

DIGITALIZZAZIONE E INNOVAZIONE TECNOLOGICA

Framework della Sicurezza informatica e della protezione dei dati per gli Istituti fisioterapici ospitalieri (IFO)

Anche in ambito sanitario, come quello finanziario e di security, sta assumendo sempre più rilevanza la necessità di attuare misure organizzative e tecnologiche adeguate a mitigare i rischi derivanti da attacchi informatici.

Il contesto internazionale propone sempre con maggiore frequenza attacchi cibernetici mirati a interrompere l'erogazione di servizi essenziali o ad entrare in possesso dei dati personali/sensibili dei cittadini, ne è esempio l'attacco hacker nel 2017 al sistema nazionale della sanità britannica ovvero il data breach che ha interessato gli USA nel 2018 e cha ha colpito un'importante struttura sanitaria e il più grande laboratorio di analisi del Paese.

Per far fronte alla crescente minaccia occorre attuare iniziative che consolidino la sicurezza del sistema informatico degli IFO e consentano di assicurare un adeguato livello di protezione dei dati e delle apparecchiature sanitarie.

In linea con quanto previsto dal quadro normativo nazionale (Piano triennale dell'informatica nella Pubblica amministrazione, Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Direttiva Nis, …) è stato ideato il framework di riferimento che, ispirato al Cybersecurity Framework del NIST (National Institute of Standards and Technology), costituisce lo strumento operativo di riferimento per organizzare il Sistema di gestione della sicurezza (SGSI) all'interno dell'Azienda.

Il framework prevede, in particolare, di implementare un SGSI in un orizzonte temporale di 36 mesi, adottando misure che possono essere sintetizzati in 4 prospettive fondamentali:

- analisi e indirizzo, per supportare la definizione dei processi, lo sviluppo di metodologie e di metriche valutative per il governo del sistema;
- iniziative di formazione e comunicazione, per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza (awarness) e competenza all'interno degli Istituti attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.
- interventi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza quali ad es. analisi delle minacce e delle vulnerabilità, monitoraggio dei bollettini e delle segnalazioni di sicurezza, implementazione e gestione di basi di dati informative;
- interventi reattivi, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e la risoluzione degli incidenti di sicurezza all'interno del dominio degli istituti;

Le azioni si declinano in interventi da attuare necessariamente a diversi livelli distinguendo tra sicurezza organizzativa, logica e fisica per incrementare la capacità di resilienza del sistema nel suo complesso. Risulta peraltro opportuno che le soluzioni di sicurezza adottate (tecnologica, organizzativa e logistica) in tema di strutture informative risultino quanto più armoniche ed omogenee possibile con quelle assunte o da assumere in materia di protezione dei dati personali al fine di rendere il sistema flessibile ed idoneo per gli scopi assegnati.

Da un punto di vista organizzativo sono da prevedere misure di prevenzione atte a ridurre il rischio di attacchi cibernetici anche con l'adozione di policy finalizzate a far assumere maggiore consapevolezza dei rischi derivanti da comportamenti non adeguati e comunque non in linea alle policy aziendali.

La sensibilizzazione sarà attuata attraverso momenti di formazione in aula, erogazione di specifici corsi e-learning e consultazione sistematica delle piattaforme rese disponibili a livello nazionale e non (si fa riferimento ad esempio al National Vulnerability Database gestito tramite la piattaforma Infosec già a disposizione di tutte le amministrazioni in sola consultazione).

E' previsto inoltre di aumentare la capacità di difesa, con l'adozione di scelte architetturali volte a ridurre la "superficie di attacco" e con l'acquisizione di dispositivi hardware e software mirati ad innalzare il livello di protezione in accordo con quanto previsto dalle "Misure minime per la sicurezza ICT delle Pubbliche amministrazioni" (Circolare AgID n.2/2017 del 18 aprile 2017). Tale documento, che fornisce indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, assume carattere obbligatorio per tutte le amministrazioni, che avrebbero dovuto garantire la propria conformità al livello minimo entro il 31 dicembre 2017.

Si intende inoltre avviare una collaborazione con la struttura incardinata in AgID (Computer Emergency Readiness/Response Team, CERT-PA) e che ha il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica rivolti ad assicurare la continuità operativa nell'erogazione dei servizi essenziali anche in presenza del sistema informatico aziendale in tutte le sue componenti di natura infrastrutturale, hardware e di software nonché della disponibilità, dell'integrità e della riservatezza delle informazioni in esso gestite.

Il Framework si fonda sulle seguenti Attività (che corrispondono alle *Category* del Cybersecurity Framework NIST):

1. Asset Management
2. Risk Analysis
3. Configuration Management
4. Operational Planning
5. Piano di Formazione e di informazione
6. Interventi di prevention
7. Interventi operativi per la gestione dell'incidente

Di seguito si riporta una descrizione schematica di ciascuna attività.

1. Asset Management

Attività	1. Asset Management
Risponde alla domanda	*Cosa devo proteggere*
Oggetto	*Identificare le risorse aziendali potenziali target di attacchi cibernetici e di altro tipo: dispositivi perimetrali, hw, sw, documenti cartacei/informatici, dati applicativi*
Responsabile	*RTD*
Accountable	*CISO*
Support	*RPCT*
Consulted	*DPO*
Informed	*Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*NIST Cybersecurity Framework, COBIT, Standard ISO/IEC 27002, Standard ISO/IEC 27001:2013, , ISO/IEC 27031:2011*
Vincoli	*Condivisione degli obiettivi con il Management aziendale*
Output	*Asset Inventory, Registro dei trattamenti*

2. Risk Analysis

Attività	2. Risk Analysis
Risponde alla domanda	*Quali sono gli elementi di rischio*
Oggetto	*Individuare i rischi e le vulnerabilità per ogni risorsa precedentemente individuata. L'attenzione è rivolta alla codifica di due processi. Il primo è il Risk Assessment che è la valutazione (probabilistica) dei rischi aziendali, a questa fase segue il Risk Management che è il processo mediante il quale si sviluppano le strategie necessarie a mitigare, eliminare e monitorare i rischi.*
Responsabile	*RTD*
Accountable	*CISO*
Support	*Owner dei processi*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*IEC 31010:2019, ISO 31000:2018, ISO Guide 73:2009, ISO/IEC 27031:2011*
Vincoli	*Esecuzione dell'attività 1, Conoscenza dei processi e delle procedure aziendali*
Output	*Risk register, Registro dei trattamenti, BPIA*

3. Configuration Management

Attività	3. Configuration Management
Risponde alla domanda	*Come utilizzare al meglio le risorse*
Oggetto	*Per ogni risorsa individuare l'ambiente di utilizzo e le modalità di transizione ad altra configurazione*
Responsabile	*RTD*
Accountable	*CISO*
Support	*Owner dei processi*
Consulted	*DPO*

Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 10007:2017, ITIL, COBIT*
Vincoli	*Esecuzione dell'attività 1*
Output	*Configuration Control Process*

4. Operational Planning

Attività	4. Operational Planning
Risponde alla domanda	*Cosa faccio prima in relazione alle criticità e alle priorità della vision aziendale*
Oggetto	*Stabilire il piano di azione in relazione agli elementi raccolti nella fase precedente*
Responsabile	*RTD*
Accountable	*CISO*
Support	*Direttore Amministrativo*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO/IEC 9001:2015*
Vincoli	*Esecuzione dell'attività 1*
Output	*Baseline di Progetto*

5. Piano di Formazione e di informazione

Attività	5. Piano di Formazione e di informazione
de alla domanda	*faccio a disporre di persone adatte al raggiungimento degli obiettivi*
etto	*porre un Piano di formazione e di informazione da destinare a personale, addetti e oratori. L'analisi degli attacchi informatici rilevano come la maggior parte sia dovuta a rtamenti non adeguati da parte del personale e dalla mancanza di procedure codificate cy. La formazione e la sensibilizzazione dei dipendenti sui rischi informatici ricoprono un chiave per la prevenzione degli attacchi e possono essere attuati anche in parallelo alla ione del Modello di sicurezza.*
onsabile	*ore Amministrativo*
untable	*nsabile della formazione*
ort	*nsabile Risorse umane*
ulted	
med	*Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione tiva, Responsabile dei flussi documentali, Responsabili degli archivi*
imenti	*O 21001:2019*
oli	*ione dell'attività 1*
ut	*di Formazione e comunicazione*

6. Interventi di prevention

Attività	6. Interventi di prevention		
	Sicurezza organizzativa	**Sicurezza perimetrale**	**Sicurezza dei server**
Risponde alla domanda	*Come riduco i rischi derivanti dalla presenza quotidiana di personale, collaboratori, addetti esterni, pazienti, visitatori*	*Come riduco i rischi di inoculazione di elementi informatici potenzialmente dannosi*	*Come riduco i rischi di vulnerabilità dei sistemi server presenti nella mia organizzazione*
Oggetto	*Definire una Policy che miri, pur nel rispetto del servizio pubblico assicurato dall'Azienda, a isolare e proteggere le risorse più critiche attraverso la loro disposizione in aree di minor accesso al pubblico e ricorrendo a dispositivi anti-intrusione (anche controlli di accesso laddove necessario) per consentire il passaggio alle sole persone abilitate. Si tratta pertanto di individuare misure organizzative che diano indicazioni alla logistica per una più adeguata allocazione delle risorse (dispositivi di rete, end point, archivi di referti e di cartelle cliniche...). Saranno da studiare misure che consentano anche il monitoraggio dei parcheggi e la possibilità di consentire il parcheggio interno ai pazienti e ai loro parenti adeguatamente registrati. Rientrano in tale categoria, anche le modalità di codifica delle procedure e dei processi concernenti la sicurezza, l'individuazione di compiti e responsabilità, le misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio, allagamento, ...) o le misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari).*	*Impostare una politica tesa alla protezione del sistema informativo degli IFO da accessi non autorizzati dall'esterno, con particola riferimento al contrasto degli attacchi informatici condotti attraverso la rete Verifica delle componenti IDS e IPS per identificare e bloccare i port scan, e a componenti di proxy server e content filtering.*	*Definire Policy per la corretta gestione dei dispositivi server con particolar riferimento alle modalità di designazione degli utenti administrator, delle configurazioni più adatte per impedire l'accesso a file e applicazioni, valutare l'opportunità di disabilitare alcuni protocolli (ad es. protocollo SMB per evitare crittografie di dati da parte di utenti smaliziati), disciplinare le modalità di aggiornamento dei firmware, collocare i server in ambienti adeguati per proteggerli da accessi fisici non autorizzati e da eventuali problemi di natura ambientale/climatica.*
Responsabile	*Direttore Amministrativo*	*RTD*	*RTD*
Accountable	*Responsabile della sicurezza aziendale*	*CISO*	*CISO*
Support	*Logista*	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27032:2012*	*ISO 27001:2017, ISO/IEC 27033:2016, ISO/IEC 27036:2016*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27033:2016, ISO/IEC 27036:2016*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Piano di sicurezza, Risk Register, Registro dei trattamenti, BPIA*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*

Attività	6. Interventi di prevention		
	Sicurezza CLOUD	**Sicurezza dispositivi utente**	**Sicurezza dispositivi sanitari**
Risponde alla domanda	*Come riduco i rischi di vulnerabilità dei sistemi CLOUD*	*Come riduco i rischi di vulnerabilità dei dispositivi utente*	*Come riduco i rischi di utilizzo di applicazioni non sicure*
Oggetto	*Attuare una Policy che, sulla base delle Linee guida diramate dal CERT Nazionale, definisca le modalità operative da adittare per la scelta e l'attivazione dei servizi CLOUD. I rischi derivano dalla gestione esternalizzata di servizi/risorse e dal luogo fisico di gestione del CLOUD, per definire il quadro legislativo di riferimento. Importante la defnizione delle regole contrattuali da prevedere e le interrelazioni con l'ambito Privacy, per gli aspetti correlati alla nomina del Responsabile esterno del Trattamento. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati.*	*Impostare una politica che sia orientata a ricorrere per i sistemi utilizzati dagli utenti (pc, stampanti di rete, smartphone, tablet,...)all'installazione di Sistemi Antivirus, anche abbinati a Personal firewall, e a Sistemi Data Loss Prevention - comprendendo in essi anche il ricorso alla crittografia - e programmazione di aggiornamento e di installazione di patch.*	*Attuare una Policy per assicurare la maggior sicurezza possibile su uso e attività di manutenzione dei dispositivi, anche in relazione alle crescenti attività che vengono svolte in modalità remota. Prevedere una procedura codificata per verificare la configurazione e per assicurare il puntuale monitoraggio del dispositivo da ingresso in azienda sino alla dismissione. La Policy deve essere conforme a standard in vigore e a linea guida "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Food and Drug Administration USA) contenente aggiornamenti relativi ai requisiti di gestione della sicurezza informatica dei dispositivi medici dotati di software. In particolare, la compliance si richiede per il sistema di categorizzazione dei rischi relativi alla sicurezza informatica basato su due livelli. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati.*
Responsabile	*RTD*	*RTD*	*RTD*
Accountable	*CISO*	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione*	*Fornitori, Regione*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27040:2017, , ISO/IEC 27033:2016, ISO/IEC 27036:2016, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27031:2011, , ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*

Attività	6. Interventi di prevention	
	Sicurezza applicativa	**Sicurezza dati**
Risponde alla domanda	*Come riduco i rischi di utilizzo di applicazioni non sicure*	*Come riduco i rischi di una esflitrazione di dati da parte degli utenti interni*
Oggetto	*Impostare una politica di sviluppo software o di acquisizione software basata su attività di monitoraggio delle procedure di sviluppo/realizzazione imperniate sulla security by design (graditi ricorsi a modelli CLASP), della documentazione e delle modalità di autenticazione anche incentivando il ricorso a SPID. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati trasmessi.*	*Attivare una Policy che prevede che, per le tipologie di dati classificati o comunque ritenuti sensibili, si attui una duplicazione degli stessi. La Policy è correlata alla gestione del data breach, in generale, ed è quindi da raccordare con le misure adottate per la privacy.Gli interventi si concretizzano in una gestione del dato ridondante "mirata" e ad attuare procedure di tracciamento puntuale di accessi ai dati medesimi. Evidenti le interrelazioni con gli interventi per l'autenticazione e la profilazione degli utenti.*
Responsabile	*RTD*	*RTD*
Accountable	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione*
Consulted	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*
Riferimenti	*ISO 27001:2017, ISO/IEC 27034:2018, ISO/IEC 27031:2011, ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27033:2016, , ISO/IEC 27031:2011*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*

7. Interventi operativi per la gestione dell'incidente

Attività	7. Interventi operativi per la gestione dell'incidente		
	Detect and identification	**Incident Management**	**Follow up**
Risponde alla domanda	*Come mi attivo di fronte ad un attacco cibernetico*	*Come gestisco un attacco cibernetico*	*Come opero dopo che l'emergenza è cessata*
Oggetto	*Organizzare una Task force (SOC+Cert) per la detection ed analisi predittiva nonché per la preventiva gestione di alert che segnalano la possibilità di un attacco cibernetico. I componenti sono individuati formalmente i componenti della Task force e ad ognuno di essi è affidato un compito con le relative responsabilità. Sono peraltro dotati di dispositivi per essere immediatamente contattati 24h e per poter agire anche in remoto. E' individuata una sala regia dove convergere in caso di necessità ed una sede di backup nel caso la prima sede non sia raggiungibile.*	*Per gestione degli incidenti, si fa riferimento a qualsiasi azione mirata ad attaccare una risorsa informativa o IT dell'Azienda. A tal fine è necessario attuare una Procedura codificata che definisca le attività che la Task force debba avviare per ripristinare le condizioni di normalità nel tempo più breve possibile e ridurre l'impatto sui servizi erogati dall'Azienda, sugli stakeholder e sulla reputation dell'organizzazione. La procedura da adottare può essere una personalizzazione del Modello ITIL.* *Si auspica un accordo con AgID per disporre del supporto della struttura del Cert-PA da disciplinare in un contesto di collaborazione più ampio.*	*Definire una Policy di Lesson learned e di alimentazione delle basi dati informative di riferimento. La componente CERT relaziona il management attraverso i dati derivanti dalla detection effettuata dal SOC, rispetto a quanto accaduto evidenzia le vulnerabilità che hanno consentito all'attaccante di sfruttare le debolezze del sistema e definisce un Piano di miglioramento per mitigare i rischi derivanti dalla o dalle vulnerabilità interessate.*
Responsabile	*RTD*	*RTD*	*RTD*
Accountable	*CISO*	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione, Garante Privacy, Polizia postale*	*Fornitori, CERT-PA, Regione*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016*	*ISO/IEC 27031:2011, ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016*	*ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016, , ISO/IEC 27031:2011, , ISO/IEC 27036:2016*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1 e dell'attività 13*	*Esecuzione dell'attività 1 e dell'attività 14*
Output	*Incident Register, Convocazione Task force, Piano di emergenza*	*Incident Register, Operatività Task force, Piano di emergenza, chiusura dell'incidente, segnalazioni ad Autorità competenti*	*Piano delle Lesson Learned, Piano di Miglioramento, Piano Operativo, Piano di formazione e comunicazione*

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento in correlazione alle Attività previste dal Framework:

CODICE	MACRO OBIETTIVI
LA-SIC-1	MIGLIORARE LE CAPACITA' DI PREVENZIONE DI ATTACCHI INFORMATICI E DELLA LORO GESTIONE
LA-SIC-2	PROCEDURALIZZARE I PRINCIPALI CONTESTI OPERATIVI (AD ES. L'ACCESSO AL SISTEMA DA PARTE DI RICERCATORI) PER DEFINIRE DELLE REGOLE DI COMPORTAMENTO
LA-SIC-3	ALLINEAMENTO ALLE MISURE INDICATE DAL PIANO DELLA REGIONE
LA-SIC-4	ACQUISIRE MAGGIORE CONSAPEVOLEZZA (AWARNESS) SU RISCHI E RESPONSABILITA' DI UN COMPORTAMENTO NON APPROPRIATO

Ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-SIC-1	1. ACQUISIZIONE DI DISPOSITIVI HW E SW PER LA PREVENTION DA ATTACCHI INFORMATICI 2. PREDISPOSIZIONE DEL DOCUMENTO DI POLICY AZIENDALE	1. NOMINA DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE 2. DESIGNAZIONE DI UN CISO (CHIEF INFORMATION SECURITY OFFICER) 3. ATTIVAZIONE DI UN TEAM PER LA VERIFICA E IL MONITORAGGIO DELLE VULNERABILITA' DI SISTEMA 4. ATTIVAZIONE DI UN'UNITA' DI CRISI PER LA GESTIONE DEGLI INCIDENTI COORDINATA DAL CISO E A CUI PARTECIPA IL RESPONSABILE PER LA PROTEZIONE DEI DATI (DPO)
LA-SIC-2	1. RICORSO A SISTEMI CENTRALIZZATI DI ASSET INVENTORY E DI ASSET MANAGEMENT AND CONFIGURATION 2. EVOLUZIONE DELLA COLLABORAZIONE GIA' IN ESSERE CON MICROSOFT PER OPERATIVITA' SCCM E POTENZIAMENTO ACTIVE DIRECTORY	
LA-SIC-3	1. ALLINEAMENTO ALLE MISURE MINIME DI SICUREZZA 2. PROPOSTA DI ACCORDO CON AGID PER AVVALERSI DELLA STRUTTURA DEL CERT-PA PER LE ATTIVITA' DI PREVENZIONE 3. CERTIFICAZIONE ISO 27000 DEL SGSI 4. PREDISPOSIZIONE DI LINEE GUIDA PER MIGLIORARE LA SCRITTURA DI CAPITOLATI ED ESECUZIONE COLLAUDI	
LA-SIC-4	1. SENSIBILIZZAZIONE DIRETTA A TUTTO IL PERSONALE MEDIANTE EROGAZIONE DI SEMINARI E DI UN CORSO SU PIATTAFORMA E-LEARNING DA ACQUISIRE	

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	IMPEGNI ECONOMICI (IVA ESCLUSA)
LA-SIC-1	1. ACQUISIZIONE DI DISPOSITIVI HW E SW PER LA PREVENTION DA ATTACCHI INFORMATICI 2. MECCANISMI DI PROTEZIONE DEI DATI	• Cyber defence Primo lotto: €53.688,52 *NOTE: finanziato dalla Regione ex art. 20 L. 67/1988 (cfr. Sezione III – scheda 3).* Secondo lotto: €65.500,00 *NOTE: è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1). Il relativo finanziamento non è alla data disponibile.* • Attività per la protezione dei dati - Sistema di encription dati sensibili 32.786,89 € - Registro delle attività di trattamento 16.393,44 € - Sistema di registro log Active Directory per copia documenti sensibili, cambio psw 8.606,56 € *NOTE: finanziato dalla Regione ex art. 20 L. 67/1988 (cfr. Sezione III – scheda 3).* - Sistema di encription dati sensibili - Tutti i reparti 40.000,00 € - Registro Log management/IAM/SIEM - Tutti i reparti 130.000,00 € *NOTE: è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1).*
LA-SIC-2	1. RICORSO A SISTEMI CENTRALIZZATI DI ASSET INVENTORY E DI ASSET MANAGEMENT AND CONFIGURATION 2. EVOLUZIONE DELLA COLLABORAZIONE GIA' IN ESSERE CON MICROSOFT PER OPERATIVITA' SCCM E POTENZIAMENTO ACTIVE DIRECTORY	Unico lotto: € 49.180,33 *finanziamento da richiedere*
LA-SIC-3	1. ALLINEAMENTO ALLE MISURE MINIME DI SICUREZZA 2. CERTIFICAZIONE ISO 27000 DEL SGSI 3. PREDISPOSIZIONE DI LINEE GUIDA PER MIGLIORARE LA SCRITTURA DI CAPITOLATI ED ESECUZIONE COLLAUDI	Unico lotto: € 25.000,00 *finanziamento da richiedere*
LA-SIC-4	1. SENSIBILIZZAZIONE DIRETTA A TUTTO IL PERSONALE MEDIANTE EROGAZIONE DI SEMINARI E DI UN CORSO SU PIATTAFORMA E-LEARNING DA ACQUISIRE	Attività in coordinamento con la UOC Sviluppo Organizzativo e del Capitale Umano *(isorisorse)*

Correlate alle misure per l'attuazione del SGSI sono quelle previste per la privacy e per completare e migliorare la conformità a quanto previsto dal Regolamento (UE) 2016/679.

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento:

CODICE	MACRO OBIETTIVI
LA-PRI-1	SUPPORTARE L' AZIONE DI GESTIONE DEL REGISTRO DEI TRATTAMENTI

Ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-PRI-1	1. LINEA GUIDA SULL'APPROCCIO PRIVACY BY DESIGN E BY DEFAULT 2. POLICY AZIENDALE SULL'UTILIZZO DEI DISPOSITIVI E APPARECCHIATURE	1. COMPLETAMENTO DEL REGISTRO DEI TRATTAMENTI 2. DEFINIZIONE DELLA METODOLOGIA PER LA VALUTAZIONE DEI RISCHI E DELLA PIA DEFINIZIONE DEL TITOLARIO DEGLI ATTI COLLEGATO ALLO SCARTO DI ARCHIVIO E AL SISTEMA DEL CONTROLLO DI GESTIONE

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	COSTO
LA-PRI-1	1. LINEA GUIDA SULL'APPROCCIO PRIVACY BY DESIGN E BY DEFAULT	Inclusa all'interno del contratto di servizi gestiti dalla UOC Affari Generali e Legali

Gestione documentale e conservazione digitale

Con tale termine si intende il processo che consente, all'interno degli IFO, il tracciamento puntuale del documento dalla fase di produzione o di ricezione a quella finale di conservazione ("ciclo di vita" del documento) in conformità alla normativa vigente in materia ed in particolar modo al Codice dell'Amministrazione digitale nonché alle regole tecniche per la protocollazione e la conservazione dei documenti informatici emanate il 3 dicembre 2013.

Si tratta di due regolamentazioni innovative, soprattutto la seconda, in quanto disciplina la conservazione a norma dei documenti elettronici e la disponibilità dei fascicoli informatici, stabilendo le regole, le procedure, le tecnologie e i modelli organizzativi da adottare per la gestione di tali processi.

Nelle more dell'emanazione delle nuove linee guida, l'AgID ha previsto nel nuovo Piano Triennale la realizzazione, sulla base delle regole tecniche in vigore, di nuovi processi orientati al miglioramento dei servizi, alla trasparenza dell'azione amministrativa e alla razionalizzazione dei costi.

Gli Istituti sono già tenuti ad individuare, nell'ambito del proprio ordinamento, almeno un'Area organizzativa omogenea e il relativo ufficio di riferimento ai sensi di quanto previsto dalle Regole tecniche, nonché a individuare il Responsabile della gestione documentale (ovvero un suo vicario, per casi di vacanza, assenza o impedimento del primo), come figura organizzativa deputata alla definizione dei flussi procedurali.

Con le nuove indicazioni fornite dall'AgID è richiesto alle PA di attuare il piano di digitalizzazione dei procedimenti amministrativi, con l'approccio "full digital" assumendo come modello il Sistema Gestione dei Procedimenti Amministrativi (SGPA) pensato per garantire l'interoperabilità tra diversi sistemi e soddisfare le richieste degli utenti in modo integrato e trasparente. L'architettura SGPA è basata su tre macro livelli funzionali:

- Front-End: abilita l'opportuno canale di comunicazione e effettua l'analisi delle richieste di servizi inviandole allo strato inferiore per l'esecuzione
- Back-End: è il componente corrispondente alle macro tipologie di servizi offerti
- Datalayer: attua la virtualizzazione dello storage sia in termini di registrazioni che di sistema di servizio di conservazione

Per quanto attiene al servizio di conservazione erogato dal corrispondente sistema, il modello da adottare amplia il classico concetto basato sulla tri-ripartizione dell'archivio (corrente, deposito e storico) in quanto prevede l'invio in conservazione dei documenti digitali secondo la logica del versamento anticipato ossia quando il ciclo di vita "corrente" non è terminato (si fa l'esempio delle fatture elettroniche), recependo il modello di riferimento proposto dallo standard OAIS (ISO 14721:2003).

Gli IFO si propongono di avviare la digitalizzazione dei procedimenti in modo graduale, procedendo a riportare nel manuale di gestione le correlate misure organizzative e tecniche da adottare.

Il manuale riporta le modalità e le procedure da adottare, anche ai fini della conservazione, dei documenti informatici fornendo le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. In considerazione della mission degli IFO, la sezione più importante descrive le modalità e le procedure da adottare per il trattamento e lavorazione dei documenti sanitari, prevedendo la conservazione sostitutiva delle cartelle cliniche, con i conseguenti

risparmi derivanti per gli Istituti dal ridimensionamento delle voci di spesa per la logistica e l'organizzazione.

Giova, al riguardo, soffermarsi sull'excursus normativo che ha accompagnato e sostenuto l'evoluzione dalla previsione del ricorso alla microfilmatura alla conservazione digitale.

Già la circolare n. 61 del 19 dicembre 1986 del Ministero della sanità ha sancito dei principi basilari:

- le cartelle vengono conservate illimitatamente dopo un quarantennio in un archivio corrente
- le radiografie non rivestendo esse il carattere di atti ufficiali, si ritiene che sotto il profilo medico, medico-legale, amministrativo e scientifico possa essere sufficiente un periodo di venti anni

Il successivo Decreto Ministeriale 14 febbraio 1997 ha poi precisato:

- La documentazione iconografica può essere acquisita mediante pellicole radiografiche, supporti cartacei, supporti elettronici. Può essere detenuta in apposito locale predisposto, può essere microfilmata oppure può essere memorizzata in archivio elettronico in conformità alla direttive dell'Agenzia per l'informatizzazione della pubblica amministrazione.
- Qualunque sia la forma di archivio prescelta, la documentazione deve poter essere disponibile a richiesta per successive esigenze mediche. Tale disponibilità deve essere mantenuta per un periodo non inferiore a dieci anni per i documenti radiologici e di medicina nucleare ed a tempo indeterminato per i resoconti radiologici e di medicina nucleare (referti), salvo termini diversi stabiliti con direttive del Ministro della sanità su conforme parere del Consiglio superiore di sanità

Infine, il Decreto 179/2012 è poi intervenuto modificando l'articolo 47-bis)) del decreto-legge 9 febbraio 2012, n. 5,convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35, aggiungendo il comma 1-bis: "A decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche puo' essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche solo in forma digitale, nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82, e dal decreto legislativo 30 giugno 2003, n. 196".

Sulla questione è poi intervenuta anche AgID che ha ulteriormene chiarito (nota prot. 7396 del 16 luglio 2014) come il quadro normativo offra la possibilità alle aziende sanitarie di effettuare la conservazione solo in formato digitale e laddove la digitalizzazione della cartella clinica sia effettuata mediante scannerizzazione di un documento cartaceo non sussista alcuna necessità di conservazione dell'originale cartaceo.

In questo secondo caso, la distruzione dell'originale cartaceo deve essere autorizzata dal Ministro dei Beni Culturali che impone un periodo pari a tre anni di conservazione del cartaceo.

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento:

CODICE	MACRO OBIETTIVI
LA-DOC-1	RENDERE OPERATIVO IL SISTEMA DI CONSERVAZIONE SOSTITUTIVA
LA-DOC-2	DIGITALIZZARE GLI ATTI NEL SISTEMA DI GESTIONE DOCUMENTALE
LA-DOC-3	SUPPORTARE L' AZIONE DI MONITORAGGIO SULLE TIPOLOGIE DI ACCESSO AGLI ATTI

Di contro, ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-DOC-1	1. NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE (NOTA INVIATA A AA.GG.) 2. IDENTIFICAZIONE DEI DOCUMENTI DA CONSERVARE, COMPRESE LE FATTURE ELETTRONICHE E LE CARTELLE CLINICHE (LETTERA AGID DEL 1 LUGLIO 2014) 3. PREDISPOSIZIONE DEL MANUALE DI CONSERVAZIONE 4. CONSERVAZIONE A FORNITORE ESTERNO QUALIFICATO	1. NOMINA DEL RESPONSABILE PER LA GESTIONE DEI FLUSSI DOCUMENTALI 2. PREDISPOSIZIONE DEL MANUALE DI GESTIONE DEGLI ATTI 3. DEFINIZIONE DEL TITOLARIO DEGLI ATTI COLLEGATO ALLO SCARTO DI ARCHIVIO E AL SISTEMA DEL CONTROLLO DI GESTIONE 4. AVVIO PROCEDURA CON MINISTERO DEI BENI E ATTIVITA' CULTURALI AL FINE DI CONSEGUIRE L'AUTORIZZAZIONE ALLA DISTRUZIONE DELLE CARTELLE CLINICHE CARTACEE CHE SONO STATE DEMATERIALIZZATE E POSTE IN CONSERVAZIONE SOSTITUTIVA (*nota prot. nr. 15099 del 07/11/2019*)
LA-DOC-2	1. ATTIVARE NUOVA RELEASE DELL' APPLICATIVO FOLIUM	
LA-DOC-3	1. ATTIVARE IL REGISTRO VIRTUALE DEGLI ACCESSI (AI FINI 241/90, CIVICO E GENERALIZZATO)	

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	IMPEGNI ECONOMICI (IVA ESCLUSA)
LA-DOC-1	1. CONSERVAZIONE A FORNITORE ESTERNO QUALIFICATO	€ 100.000,00 *NOTE: La stima economica è stata effettuata considerando un'esigenza di conservazione pari a oltre 10.000 GB l'anno* *finanziamento da richiedere*
LA-DOC-2	1. ATTIVARE NUOVA RELEASE DELL'APPLICATIVO FOLIUM E CIVILIA	€ 95.000,00 *NOTE: è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1).* *Il relativo finanziamento non è alla data disponibile.*

Comunicazione istituzionale

Con tale termine si intende il processo che consente, all'interno del'Area Organizzativa Omogenea degli IFO, il tracciamento puntuale del documento dalla fase di produzione o di ricezione a quella finale di conservazione ("ciclo di vita" del documento) in conformità alla normativa vigente in materia ed in particolar modo al Codice dell'Amministrazione digitale nonché alle regole tecniche per la protocollazione e la conservazione dei documenti informatici emanate il 3 dicembre 2013.

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento:

CODICE	MACRO OBIETTIVI
LA-COM-1	MIGLIORARE L'INTERAZIONE CON I CITTADINI PROMUOVENDO I SERVIZI OFFERTI DAGLI IFO
LA-COM-2	INCENTIVARE LE ATTIVITA' DI RICERCA
LA-COM-3	MIGLIORARE IL BENESSERE ORGANIZZATIVO COME LEVA PER INCREMENTARE LA PRODUTTIVITA'

Di contro, ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-COM-1	1. NUOVI SERVIZI ALL'UTENZA RICORRENDO ALLE TECNOLOGIE EVOLUTE: NUOVA APP IFO CON PRENOTAZIONE PRESTAZIONI, INTEGRAZIONE RECUP CONSENSO INFORMATICO AGENDA IN MEDICINA NUCLEARE TRAMITE NOTIFICHE SMS 2. MIGLIORARE LA SEZIONE DELLE PRESTAZIONI OFFERTE MIGLIORANDO LE MODALITA' DI PAGAMENTO E ATTIVANDO MODALITA' INTERATTIVE CON L'UTENZA	1. PREVEDERE CORSI DI FORMAZIONE PER IL PERSONALE INFORMATICO PER FAR FRONTE ALLE NUOVE ESIGENZE DI SVILUPPO 2. CONDIVIDERE IL FLUSSO CON LE DIREZIONI SANITARIE E CON L'UFFICIO STAMPA 3. CONDIVIDERE CONTENUTI CON LE AZIENDE OSPEDALIERE CON LE QUALI ESISTONO ACCORDI DI COLLABORAZIONE 4. RIDISEGNARE I FLUSSI DI PUBBLICAZIONE PER ELIMINARE LE ATTUALI RIDONDANZE
LA-COM-2	1. SVILUPPARE UNA SEZIONE DEL SITO AZIENDALE CON FOCUS SULLA RICERCA SCIENTIFICA	
LA-COM-3	1. INTEGRAZIONE INTRANET CON INTERNET	

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	IMPEGNI ECONOMICI (IVA ESCLUSA)
LA-COM-1	1. NUOVI SERVIZI ALL'UTENZA RICORRENDO ALLE TECNOLOGIE EVOLUTE: NUOVA APP IFO CON PRENOTAZIONE PRESTAZIONI, INTEGRAZIONE RECUP CONSENSO INFORMATICO AGENDA IN MEDICINA NUCLEARE TRAMITE NOTIFICHE SMS 2. MIGLIORARE LA SEZIONE DELLE PRESTAZIONI OFFERTE MIGLIORANDO LE MODALITA' DI PAGAMENTO E ATTIVANDO MODALITA' INTERATTIVE CON L'UTENZA	• Agenda medicina nucleare: € 12.000 *Servizio già acquisito* • Primo lotto (APP per consenso informato): €39.840,32 *NOTE: l'Attività è già inserita nel piano triennale 2017-2019 ed approvata dalla Regione Lazio con nota prot.n. 104865 del 08/02/2019. Il relativo finanziamento non è alla data disponibile.* • Secondo lotto (APP integrata con RECUP per moduli prenotazione sia in regime ordinario che in ALPI, ivi incluso il modulo di pagamento on line e l'interfaccia con i totem presenti in IFO): € 60.000,00 *finanziamento da richiedere*
LA-COM-2	1. SVILUPPARE UNA SEZIONE DEL SITO AZIENDALE CON FOCUS SULLA RICERCA SCIENTIFICA	€ 20.000,00 *finanziamento da richiedere*
LA-COM-3	1. INTEGRAZIONE INTRANET CON INTERNET	€ 20.000,00 *finanziamento da richiedere*

Digitalizzazione dei processi interni e di back office

Nel nuovo triennio è previsto l'avvio di ulteriori progetti di digitalizzazione relativi ai processi interni e di back office.

In particolaree, gli interventi interesseranno il settore contabile e quello della gestione delle risorse umane.

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento:

CODICE	MACRO OBIETTIVI
LA-BO-1	MIGLIORARE IL SUPPORTO ALLE ATTIVITA' CONTABILI
LA-BO-2	MIGLIORARE LA GOVERNANCE DELLE RISORSE UMANE

Di contro, ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-BO-1	1. SOSTITUZIONE DEL SISTEMA AMMINISTRATIVO CONTABILE	1. GOVERNANCE DELL'INTRODUZIONE DEL NUOVO SISTEMA CONTABILE CENTRALIZZATO DELLA REGIONE LAZIO
LA-BO-2	1. ACQUISIZIONE DI UNA PIATTAFORMA DI PERFORMANCE MANAGEMENT CONNESSA ALL'ORGANIGRAMMA AZIENDALE E AL SISTEMA DI VALUTAZIONE DELLE COMPETENZE GIA' IN DOTAZIONE, FINALIZZATO ALLA VALUTAZIONE ORGANIZZATIVA ED INDIVIDUALE 2. RILEVAZIONE PRESENZE E GESTIONE CARTELLINO 3. INFORMATIZZAZIONE DEL FASCICOLO DEL PERSONALE 4. INTERNALIZZAZIONE DEL SISTEMA D GESTIONE DELLE RISORSE UMANE (IVI COMPRESO ECONOMICO E GIURIDICO)	

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	IMPEGNI ECONOMICI (IVA ESCLUSA)
LA-BO-1	1. SOSTITUZIONE DEL SISTEMA AMMINISTRATIVO CONTABILE	€ 612.270,83 *finanziamento da richiedere o adesione gara regionale (SIUC)*
LA-BO-2	1. ACQUISIZIONE DI UNA PIATTAFORMA DI PERFORMANCE MANAGEMENT CONNESSA ALL'ORGANIGRAMMA AZIENDALE E AL SISTEMA DI VALUTAZIONE DELLE COMPETENZE GIA' IN DOTAZIONE, FINALIZZATO ALLA VALUTAZIONE ORGANIZZATIVA ED INDIVIDUALE 2. RILEVAZIONE PRESENZE E GESTIONE CARTELLINO 3. INFORMATIZZAZIONE DEL FASCICOLO DEL PERSONALE 4. INTERNALIZZAZIONE DEL SISTEMA D GESTIONE DELLE RISORSE UMANE (IVI COMPRESO ECONOMICO E GIURIDICO) 5. GESTIONE TURNI INFERMIERI	• Piattaforma di performance management: € 60.000,00 *finanziamento da richiedere* • Rilevazione presenze e gestione cartellino: € 55.000,00 *finanziamento da richiedere* • Fascicolo personale: € 96.573,83 *finanziamento da richiedere* • Internalizzazione del sistema di gestione delle risorse umane: €346.244,17

		• Gestione turni infermieri: è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 cfr. Sezione III – Scheda 1

Potenziamento infrastrutturale

Con tale termine si intende il processo che consente, all'interno del'Area Organizzativa Omogenea degli IFO, il tracciamento puntuale del documento dalla fase di produzione o di ricezione a quella finale di conservazione ("ciclo di vita" del documento) in conformità alla normativa vigente in materia ed in particolar modo al Codice dell'Amministrazione digitale nonché alle regole tecniche per la protocollazione e la conservazione dei documenti informatici emanate il 3 dicembre 2013.

Di seguito si riepilogano i macro-obiettivi delle azioni da attuare nel triennio di riferimento:

CODICE	MACRO OBIETTIVI
LA-INF-1	AMMODERNAMENTO DELL'ASSET TECNOLOGICO
LA-INF-2	ESTENSIONE WI-FI
LA-INF-3	RIDUZIONE COSTI DI TELEFONIA

Di contro, ciascun macro-obiettivo si declina nelle seguenti attività:

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	ATTIVITA' ORGANIZZATIVE
LA-INF -1	ACQUISIZIONE NUOVE APPARECCHIATURE	
LA-INF -2	1. ESTENSIONE WI-FI (GUEST – DOMINIO) 2. DEFINIZIONE PASSWORD POLICY E GESTIONE DELLE UTENZE GUEST E DI DOMINIO	
LA-INF-3	POTENZIAMENTO TOIP E MODULO FAX SERVER	

Valutazione costi

CODICE	ATTIVITA' IN CARICO A UOSD TECNOLOGIE	IMPEGNI ECONOMICI (IVA ESCLUSA)	
LA-INF -1	ACQUISIZIONE NUOVE APPARECCHIATURE	• Switch HPE: € 45.000,00 • PDL n. 250 + Portatili 50: € 175.000,00 • N. 180 Access Point wifi interfacciabili con Firewall Aziendale: €72.000 • Sistemi Backup offline e VTL:: € 90.000,00 • Lavori accessori: € 265.000	*è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1).*
		• Dischi blade e altre app.re: € 35.459,70	Budget *Conto Patrimoniale*
		• Nr. 4 sistemi di videoconferenza: € 8.196,72 • Sistemi NAS per archiviazione dati: € 8.196,72	*finanziato dalla Regione ex art. 20 L. 67/1988 (cfr. Sezione III – scheda 3).*
		• Server blade: € 500.000,00 • Nr. 6 sistemi di videoconferenza: € 30.000,00 • Sistemi NAS per archiviazione dati: € 40.000,00 • Lavori accessori: € 80.000	*è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 2).*

LA-INF -2	ESTENSIONE WI-FI (GUEST , DOMINIO)	€ 72.000,00 *è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1)*
LA-INF-3	POTENZIAMENTO TOIP E MODULO FAX SERVER	€ 60.000,00 *finanziamento da richiedere*

SEZIONE II:

SANITA' DIGITALE

Cartella Clinica elettronica (CCE) di reparto ed ambulatoriale

La digitalizzazione della Cartella Clinica costituisce uno degli obiettivi strategici degli IFO. Sono state già avviate le attività prodomiche, elaborando il report dei reparti che ad oggi utilizzano la cartella clinica ed il diagramma di flusso di funzionamento della stessa cartella clinica con l'analisi delle criticità e con le operazioni ad oggi in atto per risolverle.

La cartella clinica ambulatoriale invece è stata installata come ambulatorio pilota presso ortopedia oncologica con esito positivo di utilizzo.

È stato quindi redatto un piano attuativo di realizzazione su 4 steps che prevedono nel dettaglio:

1 step: attivazione della CCE ambulatoriale su 12 ambulatori dei 25 totali in IFO.

In questo primo step verrà creata la CCE ambulatoriale "base" che potrà essere applicata su 12 ambulatori degli IFO. In 4 dei 12 ambulatori la stessa verrà completamente verticalizzata entro il 31/12/2019 per poi procedere nei primi mesi del 2020 alla verticalizzazione dei restanti 8 ambulatori. Il tutto verrà costantemente seguito ed approvato da un gruppo di lavoro operativo della Direzione Sanitaria Aziendale che lavorerà a stretto contatto con la UOSD Tecnologie e Sistemi Informatici.

2 step: avvio in febbraio 2020 e conclusione nel Marzo 2021, vede la realizzazione della CCE nei restanti 13 ambulatori. In questo periodo verranno verticalizzate tutte le CCE in esame e saranno supportate da una infrastruttura di rete adeguata, realizzata con il precedente piano triennale (Wi-Fi, bonifica armadi rack, ricamblaggio strutturato, TOIP e potenziamento segnale voce e dati).

3 step: avvio in aprile 2021 e conclusione nell'ottobre 2021 prevede la realizzazione e la verticalizzazione della CCE in 12 reparti. Il tutto sempre con la collaborazione del gruppo di lavoro operativo della Direzione Sanitaria Aziendale che lavorerà a stretto contatto con la UOSD Tecnologie e Sistemi Informatici.

4 step: conclusione atività nel periodo novembre – dicembre 2021 con la realizzazione e verticalizzazione della CCE nei restanti 4 reparti degli IFO.

Scheda costi e copertura economica

Descrizione attività	Costo stimato IVA esclusa	Copertura finanziaria
1 step	39.477,87 €	Budget 2019 da collaudare e fatturare entro il 31/12/2019
2 step	81.967,21 €	Approvati con nota Regione Lazio prot.n.104865 del 08/02/2019
3 step	81.967,21 €	Richiesta alla Regione Lazio con nota prot.n.9144 del 01/07/2019
4 step	48.848,57 €	Budget 2020

Nel periodo 2021-2023 è previsto il potenziamento della cartella clinica digitale di reparto con il modulo relativo alla gestione completamente in digitale della terapia farmacologica, ed interfaccia diretta con la farmacia ospedaliera.
La spesa prevista è di € 120.000,00 oltre IVA : è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020 (cfr. Sezione III – scheda 1).

Monitoraggio dei PDTA – Data warehouse – Business Intelligence

Con il DM 12 marzo 2019 "Nuovo sistema di garanzia per il monitoraggio dell'assistenza sanitaria" (di seguito, *NSG*) pubblicato in G.U. il 14 giugno 2019, è stato introdotto un nuovo strumento (operativo dal 1° gennaio 2020) che consente, a partire dai dati desumibili dal Sistema Informativo Ospedaliero (NSIS), la misurazione secondo le dimensioni dell'equità, dell'efficacia, e della appropriatezza delle prestazioni erogate.

Il *NSG* si articola in un insieme di indicatori relativi ai tre macro-livelli di assistenza (prevenzione collettiva e sanità pubblica; assistenza distrettuale; assistenza ospedaliera) e prevede il monitoraggio e la valutazione dei percorsi diagnostico-terapeutico-assistenziali (PDTA) per specifiche categorie di bisogni o condizioni di salute. La valutazione dei PDTA a livello regionale e nazionale deve essere effettuata in termini di appropriatezza, esito clinico, equità ed impatto economico.

L'obiettivo generale è quello di confrontare i diversi modelli assistenziali per le patologie croniche ed acute allo scopo di identificare la strategia migliore in termini di efficacia (effectiveness), costo-efficacia (cost-effectiveness) e sostenibilità economica.

In tale contesto assume una rilevanza strategica poter assicurare il monitoraggio puntuale dei PDTA e disporre di dati che, attraverso anche il recupero del pregresso, possa consentire di effettuare delle previsioni sull'efficacia degli stessi in base a specifici algoritmi predittivi.

La nuova impostazione determina, di conseguenza, la necessità, a fronte del tracciamento di ogni fase di ciascun PDTA, di implementare strumenti di business intelligence ricorrendo anche alle innovative soluzioni fornite dall'Intelligenza Artificiale.

IFO, consapevole della sua *mission* orientata all'assistenza di pazienti per lo più fragili dalle patologie spesso croniche, intende attuare un sistema di gestione del percorso assistenziale innovativo appropriato alle specifiche esigenze dell'assistito attraverso un approccio interdisciplinare che colloca il paziente al centro del sistema. Da tale approccio l'analisi dei Percorsi Paziente-centrici che derivano dal nuovo approccio possono determinare anche nuove metodologie di cure personalizzate in coerenza con la caratteristica di IRCCS degli Istituti, che se confortate dagli esiti potrebbero poi dare adito all'individuazione di nuovi pattern da inserire nelle metodologie standard, secondo un approccio PDCA mirato ad assicurare una sempre più appropriata qualità delle prestazioni assistenziali. Da qui la necessità di avvalersi di sistemi di business intelligence per analizzare la gran mole di dati che è associata a ciascun percorso di cura e progettare nuovi percorsi di riferimento attraverso analisi predittive che consentano di valutare le più adeguate risorse necessarie e la migliore qualità attesa attraverso la WHAT IF analysis.

Data warehouse, business intelligence e Intelligenza artificiale diventano quindi strumenti indispensabili per le scelte di politica sanitaria, consentendo di monitorare e governare i processi ospedalieri evidenziandone criticità e permettendo di attuare misure di efficientamento: peraltro il loro utilizzo sarà finalizzato a supportare le attività di ricerca, e in particolare per analizzare dati assistenziali dal punto di vista epidemiologico, statistico, e di ricerca nonché a dare evidenza del rapporto costi/efficacia dei farmaci.
Il progetto, fortemente sostenuto dalla Direzione IFO, si attuerà attraverso una introduzione di un sistema di monitoraggio per un numero ristretto e circoscritto di PDTA correlate al sistema del RIS-PACS, per poi estendersi agli altri secondo un approccio graduale che tenga conto delle contemporanee attivazioni delle cartelle cliniche di reparto, del referto digitale e delle altre innovazioni di processo.

I costi di sviluppo presunti sono di € 65.000 per il primo anno e di 40.000 dal secondo anno in poi, in carico ad IFO.

Processo digitalizzato di consenso Informato e consenso al trattamento dei dati sensibili

Oggi, tutte le informazioni necessarie ad un paziente per decidere se sottoporsi a un atto sanitario, se e perché rilasciare il consenso al trattamento dei dati sensibili, sono comunicate dal medico tramite colloquio, con il supporto di ausili tradizionali come libretti, brochure. È noto che una parte delle cause medico-legali che vengono intentate contro le strutture ospedaliere e il personale sanitario sono motivate dal fatto che i pazienti non hanno compreso a fondo tutti i rischi e le conseguenze che il medico ha loro spiegato. Oltre a questo ci sono altri aspetti da considerare, come ad esempio il volume di carta che il processo di acquisizione dei consensi genera, gli obblighi di conservazione imposti dalle normative e infine la tracciabilità della documentazione in relazione con la cartella clinica. Obiettivo degli IFO è quello di digitalizzare completamente il processo affiancando il medico e la struttura sanitaria nell'erogazione del consenso informato al paziente, rispettando tutte le norme vigenti e certificando la comprensione da parte del paziente. Il tutto attraverso un applicativo raggiungibile dal paziente sia su Tablet fornito dagli IFO che su smartphone o pc direttamente da casa del paziente stesso. Attraverso questo applicativo il paziente avrà a disposizione video, testi ed immagini esplicative e rialscerà i suoi consensi attraverso un piccolo questionario di autoapprendimento e firma grafometrica. Tali consensi si interfacceranno con i sistemi digitali aziendali come la Cartella Clinica Elettronica, il RIS-PACS, il LIS (Laboratorio analisi), il sistema di anatomia patologica, l'anagrafica aziendale, i laboratori di ricerca, ecc… garantendo la privacy desiderata dal paziente.

L'applicativo prevede, inoltre, meccanismi di firma elettronica avanzata (FEA) e qualificata (FEQ) per digitalizzare l'intero processo conformemente alle indicazioni fornite dall'Agenzia per l'Italia digitale (AgID).

Da non sottovalutare i riflessi sulla reputation dell'Azienda, considerato che l'effetto secondario è quello di aumentare il grado di convolgimento del cittadino nei processi sanitari, migliorare le performance in termini di riduzione di sprechi e di tempo, ridurre i contenziosi con l'azienda.

I costi di sviluppo di questo sistema per n.10 punti firma sono stati completamente inclusi nel budget 2020. Per il 2021 è prevista la progressiva estensione ad altri reparti/ambulatori per un costo pari ad € 32.786,98 finanziati con III Fase art. 20 L.67/88 (cfr. Sezione III – scheda 3) e per il completamento delle attività nel biennio il costo previsto è di 90.000 (cfr. Sezione III – scheda 1).

Digitalizzazione del processo chirurgico ivi compresa la preospedalizzazione

In merito alla digitalizzazione del percorso chirurgico nel corso del 2019 è stato completato l'intero iter di sala operatoria garantendo il completo paperless. L'agenda operatoria ed il registro operatorio sono ad oggi completamente digitali in tutte le loro interfacce: chirurghi, infermieri ed anesteisti. È stato completamente digitalizzato anche il percorso di preospedalizzazione anestesiologica.

Nel piano precedente ci si era posti questo obiettivo, raggiunto, mentre nell'attuale piano per la transizione digitale ci si pone un secondo obiettivo:

- digitalizzare completamente la lista di attesa per accesso alla pre-ospedalizzazione e completamento di quest'ultima ad oggi attiva solo per la parte anestesiologica. Tale attività procede di pari passo con lo sviluppo della cartella clinica elettronica ambulatoriale;

- digitalizzare anche la firma del verbale operatorio che invece può realizzarsi solo con lo sviluppo totale della cartella clinica elettronica di reparto.

I costi di sviluppo di questo sistema sono stati già inclusi nel budget 2021, all'interno delle classiche giornate di sviluppo previste nel contratto di manutenzione, per € 45.000,00.

Prescrizione/ricette dematerializzate

Nel corso del 2016 la Regione Lazio ha introdotto la ricetta dematerializzata sia per le prescrizioni farmaceutiche che per le specialistiche, mettendo a disposizione delle Aziende Sanitarie il software denominato Mesir e consentendo così, dall'ottobre dello stesso anno, la trasmissione della ricetta direttamente al MEF. In questo processo è stato introdotto il CUR (Catalogo Unico Regionale) che aggancia tutte le prestazioni presenti nel tariffario regionale ad oggi in vigore ai codici unici Regionali e Nazionali. Oltre alle attività di formazione, è stato anche effettuato un lavoro di collegamento tra le prestazioni erogate dai nostri ambulatori/servizi ed i codici del CUR.

Nel precedente piano del'informatizzazione è stato acquisito il sistema di prescrizione/ricette dematerializzate. L'avvio dello stesso è funzionale all'avvio della CCE sia ambulatoriale che di reparto e consentirà nel prossimo triennio di:

- generare prescrizioni specialistiche (autoimpegnative) in modalità dematerializzata
- prendere in carico di una ricetta dematerializzata, passaggio obbligatorio per accogliere un paziente durante una prenotazione ReCUP o una accettazione diretta
- erogare una ricetta dematerializzata precedentemente presa in carico dal ReCUP o dalla accettazione ambulatoriale.

I costi di sviluppo di questo sistema sono inclusi nel budget 2021, all'interno delle classiche giornate di sviluppo previste nel contratto di manutenzione per € 17.000,00

Sistema digitale ed interattivo con il paziente per la prenotazione esami Medico Nucleare

E' previsto l'accesso all'applicazione da parte del personale medico e sanitario degli I.F.O. e di tutte le altre strutture esterne (ASL, Aziende Ospedaliere, Policlinici Universitari, ecc…).

Una volta registrati, i medici (sia interni agli IFO che esterni) possono inserire le richieste di esami per i propri assistiti compilando un'apposita form: la richiesta di esame è esaminata dal Personale medico/sanitario che, una volta verificata la completezza dei dati e la tipologia di prestazione, propone, in caso di verifica positiva, una data in relazione alla disponibilità in agenda. All'assistito è inviata una notifica via sms, mediante la quale l'utente può gestire in modo interattivo e direttamente il suo appuntamento, confermandolo, ripianificandolo ovvero annullandolo.

E' previsto anche l'avvio di un sistema di recall.

Alla fase sperimentale iniziata nel 2019, segue nel triennio il completamento dell'estensione.

I costi di sviluppo del sistema sono stati coperti con un anticipo sul finanziamento richiesto in Regione Lazio non ancora erogato e pari ad € 36.000,00. I successivi costi (10%) sono relativi alla sola gestione del sistema sul budget 2021 per € 3.600,00.

Per quanto riguarda il sistema di recall è previsto un costo per il 2021 di € 9.837 (finanziati con III Fase art. 20 L.67/88, cfr. Sezione III – scheda 3) e per il completamento nel successivo biennio di € 50.500 (è stato richiesto il finanziamento alla Regione con nota prot. nr. 839320 del 30 settembre 2020, cfr. Sezione III – scheda 2).

Sistema di cartella clinica e gestione percorso paziente per i trattamenti radioterapici

Il progetto del nuovo Sistema Gestionale per la Radioterapia Oncologica (Speed RO) ha come obiettivo la realizzazione della meta cartella del paziente, il miglioramento della fruibilità delle informazioni all'interno del Reparto, l'incremento della performance individuale del personale medico, il supporto al personale nella produzione dei report e nelle statistiche.

In particolare, il nuovo sistema consente:

- l'acquisizione del codice univoco (MPI) del paziente per disporre di un unico sistema di identificazione, favorendo l'interoperabilità con gli altri applicativi gestionali degli IFO;

- al CUP regionale la consultazione delle date di appuntamento per le prime visite e i follow Up

- l'acquisizione automatica delle prestazioni erogate e il controllo automatizzato della congruità e del regime di ricovero per la contabilizzazione interna e la produzione delle impegnative SSN

- la produzione dematerializzata delle impegnative SSN e dei flussi informativi interni per i riscontri amministrativi;

- la dismissione dell'applicativo DBRAD (software di realizzazione interna agli IFO)

- la gestione della chiamata anonima dei pazienti in sala d'attesa.

La soluzione individuata prevede, inoltre, la fornitura anche dell'hardware necessario all'utilizzo del sistema presso il Reparto di Accettazione e della Sala di attesa come di seguito precisato:

una postazione per le attività di Accettazione (Check-in) con Zebra Kiosk da muro

un monitor HDMI 15"

uno scanner barcode per le tessere sanitarie dei pazienti

una stampante Zebra KR403 ethernet di ticket su carta termica con taglierina automatica dotata inoltre di un alloggiamento per rotoli di carta di grandi dimensioni per una maggiore autonomia.

un televisore LED 42" con ingresso HDMI per le chiamate ai servizi; un

Il nuovo modulo acquisito nel corso del 2019 permetterà inoltre l'interoperabilità di Speed RO con altri applicativi sanitari operanti presso gli Istituti e con gli applicativi regionali consentendo:

a) l'integrazione con il Sistema Informativo Ospedaliero per la ricezione (inserimento, aggiornamento e merge) dell'anagrafica centralizzata del paziente e del corrispondente codice MPI (Master Patient Index).

b) l'integrazione con il CUP Regionale, al fine di ricevere gli appuntamenti di Prima Visita e Follow Up. A tal fine saranno utilizzate le tabelle di frontiera messe a disposizione da ReCup.

c) l'integrazione con ARIA® in modo tale che siano automaticamente acquisite da ARIA® gli appuntamenti del ReCup e le relative anagrafiche dei pazienti e le rendicontazioni attività

d) la produzione delle impegnative del SSN direttamente con il MEF o attraverso la componente del software Dedalus.

Sono state realizzate:

- le specifiche d'interscambio del codice MPI con People di Dedalus;

- la procedura di estrazione da DB delle date degli appuntamenti dalle agende di VARIAN;

- la visibilità degli appuntamenti di radioterapia in tabelle di frontiera a disposizione del CUP Regionale;

- procedura di acquisizione automatica delle prestazioni erogate e controllo automatizzato della congruità per la contabilizzazione interna e la produzione delle impegnative SSN VARIAN

- Produzione reportistica automatica per la fornitura degli elenchi mensili delle prestazioni erogate (suddivise per medico-paziente) di cui si devono manualmente prescrivere le impegnative SSN;

Ad oggi sono in corso di realizzazione le seguenti ulteriori attività:

- realizzazione della prescrizione impegnativa SSN dematerializzata;

- installazione del modulo per la chiamata anonima in sala d'attesa;

- completamento della personalizzazione per l'implementazione dell'algoritmo di avanzamento nella lista di attesa

I costi di sviluppo di questo sistema (€ 38.800,00) sono stati completamente inclusi nel budget 2021. E' In corso l'avvio del sistema.

Realizzazione di un nuovo sistema di gestione dell'Anatomia patologica ed integrazione dello stesso al percorso clinico assistenziale digitale

Gli IFO ad oggi dispongono di un sistema informatico di Anatomia patologica che permette una interfaccia diretta con i reparti e con gli ambulatori ma, non essendo di ultima generazione, limita l'interfaccia ai più evoluti sistemi di CCE in fase di implementazione.

Per tale ragione durante il 2020 sarà necessario procedere con l'implementazione di un nuovo sistema di Anatomia Patologica in grado di interfacciarsi, attraverso un sistema di order/entry, con la CCE ambulatoriale e di reparto e permettere a tutti i medici di visualizzare con facilità ed all'interno della scheda paziente, il referto e l'immagine scansionata del vetrino analizzato.

Il progetto prevede inoltre la scansione dei vetrini ed un processo di identificazione attraverso imprinting laser sullo stesso vetrino che lo identifichi univocamente. Lo stesso metodo permetterà inoltre di trasmettere direttamente l'immagine del vetrino per una *second opinion* o in caso di ricerca scientifica.

I costi stimati per il 2021-2023 sono pari a € 30.000,00.

Progetto paperless per eliminazione dei documenti sanitari cartacei digitalizzati su conservazione sostitutiva

Gli Istituti Fisioterapici Ospitalieri (IFO) hanno avviato un percorso di graduale miglioramento dei servizi offerti all'utenza basato principalmente sulle opportunità offerte dalla digitalizzazione e dall'innovazione tecnologica: in tale ambito, assume particolare rilevanza il Progetto che può trovare una identificazione nella descrizione di "IFO Paperless" e che ispirandosi ai principi della mobile health e del full digital, si pone l'obiettivo di:

- rendere più efficienti i servizi ampliandone la diffusione
- agevolarne la governance anche dal punto di vista della privacy e della cybersecurity
- razionalizzare l'utilizzo delle risorse umane ed economiche con i conseguenti benefici in termini complessivi di miglioramento della performance aziendale.

Il progetto in parola intende porre le basi per la produzione, il trattamento e la ricezione di documenti nativi digitali in conformità alla normativa vigente in materia ed in particolar modo al Codice dell'Amministrazione Digitale (CAD) nonché alle regole tecniche per la protocollazione e la conservazione dei documenti informatici emanate il 3 dicembre 2013, nelle more dell'emanazione delle nuove linee guida sulla formazione, gestione e conservazione dei documenti informatici attualmente in fase di consultazione pubblica.

Si evidenzia che il progetto prevede l'avvio della conservazione sostitutiva della documentazione sanitaria con la conseguente dematerializzazione degli originali cartacei in funzione dell'attuazione del percorso di completa digitalizzazione dei procedimenti clinici e risparmio per gli IFO che ad oggi spendono ingenti somme per la sola conservazione fisica documentale.

A tali fini, giova ricordare che il quadro normativo e regolamentare del trattamento e conservazione della documentazione sanitaria ha subito negli anni continue evoluzioni, determinate oltre che dal CAD e dai correlati regolamenti di attuazione, anche da specifici interventi del Legislatore. Si fa riferimento, ad esempio, a:

- la Circolare n. 61 del 19 dicembre 1986 con la quale il Ministero della Sanità ha disposto la conservazione illimitata delle cartelle dopo un quarantennio in un archivio corrente e la conservazione limitata delle radiografie per un periodo di venti anni
- il Decreto Ministeriale 14 febbraio 1997 con il quale è stata introdotta la possibilità per la documentazione iconografica di essere acquisita mediante pellicole radiografiche, supporti cartacei, supporti elettronici, di essere detenuta in apposito locale predisposto, di essere microfilmata oppure di essere memorizzata in archivio elettronico in conformità alle direttive dell'Agenzia per l'informatizzazione della pubblica amministrazione. Lo stesso Decreto ha però precisato che qualunque sia la forma di archivio prescelta, la documentazione deve poter essere disponibile a richiesta per successive esigenze mediche: dieci anni per i documenti radiologici e di medicina nucleare ed a tempo indeterminato per i resoconti radiologici e di medicina nucleare (referti), salvo termini diversi stabiliti con direttive del Ministro della Sanità su conforme parere del Consiglio superiore di sanità.
- il Decreto 179/2012 che ha revisionato l'articolo 47-bis del decreto-legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35, aggiungendo il comma 1-bis: "A decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche può essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche solo in forma digitale, nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82, e dal decreto legislativo 30 giugno 2003, n. 196".

- la nota dell'Agenzia per l'Italia Digitale (AgID) prot. n. 7396 del 16 luglio 2014 con la quale è stato precisato come il quadro normativo vigente offra la possibilità alle aziende sanitarie di effettuare la conservazione solo in formato digitale e, laddove la digitalizzazione della cartella clinica sia effettuata mediante scannerizzazione di un documento cartaceo, non sussista alcuna necessità di conservazione dell'originale cartaceo fermo restando che la distruzione dell'originale cartaceo deve essere autorizzata dal Ministro dei Beni Culturali che impone un periodo pari a tre anni di conservazione del cartaceo.

Per quanto esposto, anche in considerazione dei rilevanti costi che gli Istituti sostengono per la conservazione "esternalizzata" della documentazione originale cartacea, assume carattere prioritario individuare, con la dovuta urgenza, le modalità operative che consentano agli IFO di attuare la conservazione digitale della documentazione sanitaria e, nel contempo, di procedere alla distruzione dei documenti originali dematerializzati detenuti da più di tre anni.

Per tale ragione viene avviata la fase interlocutoria con Regione Lazio, AgiD, Ministero dei Beni e delle Attività Culturali al fine di perseguire l'obiettivo della conservazione sostitutiva completamente digitale.

I costi sono stati già stimati nella sezione I.

Potenziamento infrastruttura hardware funzionale al percorso sanitario (Rete Wi-Fi, potenziamento segnale mobile voce e dati all'interno della struttura IFO, bonifica infrastruttura di rete e armadi rack, potenziamento blade già operativo e acquisto nuovo server blade)

Gli IFO hanno richiesto uno specifico finanziamento mirato all'adeguamento della infrastruttura tecnologica ancora non completata nel fase del precedente triennio.

Sono in fase di completamento:

- il sistema Wi-Fi aziendale che prevede un'estensione dello stesso ai restanti reparti e ambulatori;
- il potenziamento del segnale mobile voce e dati all'interno della struttura IFO è in fase di realizzazione e la gara d'appalto è stata aggiudicata e completata;
- è in fase di completamento la bonifica dell'infrastruttura di rete (switch ed armadi rack di piano);
- è necessario il potenziamento in termini di acquisizione di server blade dedicate alla continua crescita di uno storage locale che permetta l'archiviazione di dati sanitari e della ricerca scientifica.

I costi sono stati già stimati nella sezione I.

Disaster recovery in Cloud

Gli IFO hanno richiesto finanziamento specifico per la realizzazione del distar recovery in Cloud. Tale attività, come specificato anche nelle linee guida AgiD ed al c. 3, lettera b) dell'art. 50 bis del Codice dell'Amministrazione Digitale, diventa fondamentale nella gestione in sicurezza dei propri dati e nell'ambito della continuità di esercizio.

Il CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi (art. 15 "Digitalizzazione e riorganizzazione"). Da tale indicazione consegue, per la Pubblica Amministrazione (nel prosieguo PA), anche l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese. Questa affermazione assume particolare significato a fronte del sempre maggiore utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti, che rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità dei dati. Quando i dati, le informazioni e le applicazioni che li trattano sono parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali di un ente/organizzazione, diventano un bene primario per il quale è necessario garantire salvaguardia e disponibilità, anche attraverso l'adozione di misure di sicurezza e di soluzioni atte a garantire la continuità di funzionamento dei sistemi informativi.

Questo obbligo finora è stato assolto, a fronte di eventi che hanno avuto un impatto sul regolare funzionamento dell'organizzazione, ricorrendo a soluzioni di emergenza di tipo tradizionale quali: il trasferimento dei servizi presso gli uffici rimasti operativi, l'attivazione di procedure amministrative alternative, l'ausilio di personale aggiuntivo, ecc.. Oggi l'impiego di procedure alternative di tipo tradizionale è quasi sempre insufficiente a garantire la continuità dei servizi, atteso il diffuso utilizzo delle tecnologie informatiche. Anche qualora il procedimento amministrativo appaia "non informatizzato", una fase del suo procedimento è stata assolta mediante applicazioni informatiche; inconvenienti di natura tecnica, pertanto, possono condizionare il normale svolgimento dei processi tradizionali, fino a comportare il blocco delle attività istituzionali anche per lunghi periodi.

La Continuità Operativa ICT obiettivo del prossimo triennio, riguarda il processo critico ICT che, nel caso di grave e prolungata indisponibilità dei sistemi informativi (disservizio incompatibile con le esigenze di continuità di funzionamento dell'Amministrazione), prevede anche il Disaster Recovery per garantire il ripristino dello stato del Sistema Informativo (o di parte di esso), per riportarlo alle condizioni di funzionamento e di operatività antecedenti all'evento disastroso.

I costi di impianto per il primo anno sono pari a € 186.065,57, di cui € 150.000 per start-up, finanziati con III Fase art. 20 L.67/88 (cfr. Sezione III – scheda 3) e per le attività di gestione nei due anni successivi l'importo previsto è di 381.000 (cfr. Sezione III – scheda 2).

Semplificazione della procedura di richiesta di invalidità civile – INPS

A decorrere dall'1.1.2010 le domande di accertamento invalidità civile, cecità civile, sordità civile, handicap e disabilità dovranno essere trasmesse per via telematica all'I.N.P.S. dal diretto interessato o dagli Enti di Patronato/Autorizzati o Associazioni di Categoria ai sensi della Legge n. 102 del 3 agosto 2009.

Affinché la domanda sia acquisita regolarmente dalla procedura Inps è necessario che il medico curante abbia trasmesso telematicamente il certificato con l'indicazione delle patologie per cui si richiede il riconoscimento, consegnandone una copia cartacea debitamente firmata, all'interessato.

In caso di richiesta di visita domiciliare il certificato medico telematico allegato alla domanda dovrà attestare l'assoluta in trasportabilità del richiedente. Il parametro dell'intrasportabilità deve essere riferito al complesso e alla gravità delle situazioni cliniche in atto, che rendono rischioso e pericoloso per il paziente o per gli altri lo spostamento dello stesso e non deve essere inteso come puro fatto fisico legato alla capacità di deambulare. Qualora sussistano le condizioni per richiedere la visita domiciliare, il medico abilitato a rilasciare il certificato la può richiedere all'inizio dell'iter o, nel caso sia stata già fissata la visita ambulatoriale, deve compilare ed inviare (sempre per via telematica, collegandosi al sito dell'INPS) il relativo certificato medico almeno 5 giorni prima.

La A.S.L., conclusa la procedura relativa all'accertamento sanitario dell'invalidità, trasmette il verbale alla Commissione medica di verifica I.N.P.S.

Il verbale definitivo di invalidità viene inviato dalla competente sede I.N.P.S., direttamente all'interessato con lettera raccomandata.

Al fine di semplificare tale iter per il cittadino, gli IFO sono diventati un Ente Autorizzato dall'INPS per l'effettuazione di quanto esposto precedentemente e cioè della redazione completa e diretta dell'accertamento sanitario da inviare alla commissione medica di verifica INPS.

I costi del progetto non sono in carico agli IFO.

SEZIONE III:

RIEPILOGO COSTI

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Scheda	Forma di finanziamento richiesto: Nota Regione Lazio prot.n. 839320 del 30/09/2020	Stato: in attesa di finanziamento	
	TECNOLOGIE INFORMATICHE	**COSTO PRESUNTO IVA ESCLUSA**	**COSTO PRESUNTO IVA INCLUSA**
	n.250 PDL e n.50 PC portatili - Tutti i reparti	175.000,00 €	
	Sistema Recall esame paziente - Tutti i reparti	10.500,00 €	
	n.6 Sistemi di videoconferenza - Dipartimenti clinici	30.000,00 €	
	Integrazione comunicazione al paziente tramite sito web - Dipartimenti clinici	40.000,00 €	
	SW per prescrizione e somministrazione farmaci con sistema informatizzato - Tutti i reparti + Farmacia	50.000,00 €	
	Upgrade Folium - Tutti i reparti / Upgrade Civiia - Tutti i reparti	95.000,00 €	
	Completamento CC Digitale Reparti - Tutti i reparti di degenza	70.000,00 €	
	Sistema di encription dati sensibili - Tutti i reparti	40.000,00 €	
	Ampliamento CONFIRMO - Tutti i reparti	90.000,00 €	
	Registro Log management/IAM/SIEM - Tutti i reparti	130.000,00 €	
1	Sistema Cyber defence - Tutti i reparti	65.500,00 €	
	Gestione turnistica infermieristica	50.000,00 €	
	TOTALE	**846.000,00 €**	**1.032.120,00 €**
	ULTERIORI TECNOLOGIE		
	n.180 Access Point Wi-Fi interfacciabili con Firewall Aziendale	72.000,00 €	
	Sistema Back up Off-line	45.000,00 €	
	Sistema di Back up VTL	45.000,00 €	
	n.30 switch HPE	45.000,00 €	
	TOTALE	**207.000,00 €**	**252.540,00 €**
	LAVORI ACCESSORI		
	Cablaggio dorsali rame, realizzazione punti rete, installazione server e storage	140.000,00 €	
	Sostituzione FO	125.000,00 €	
	TOTALE	**265.000,00 €**	**323.300,00 €**
	TOTALE COMPLESSIVO SCHEDA 1	**1.318.000,00 €**	**1.607.960,00 €**

Scheda	Forma di finanziamento richiesto: Nota Regione Lazio prot.n. 839320 del 30/09/2020	Stato: in attesa di finanziamento

	TECNOLOGIE INFORMATICHE	COSTO PRESUNTO IVA ESCLUSA	COSTO PRESUNTO IVA INCLUSA
2	Fornitura potenziamento Server Blade	500.000,00 €	
	Sistema di disaster recovery	381.000,00 €	
	NAS Archiviazione dati	40.000,00 €	
	TOTALE	**921.000,00 €**	**1.123.620,00 €**
	LAVORI ACCESSORI		
	Installazione sistemi	80.000,00 €	97.600,00 €
	TOTALE COMPLESSIVO SCHEDA 2	**1.001.000,00 €**	**1.221.220,00 €**

Scheda	Forma di finanziamento richiesto: Finanziamento ex art.20 L.67/88 III FASE	Stato: Finanziato con Determinazione Regione Lazio G14005 del 24/11/2020	
3	**TECNOLOGIE INFORMATICHE**	**COSTO PRESUNTO IVA ESCLUSA**	**COSTO PRESUNTO IVA INCLUSA**
	Sistema di disaster recovery	186.065,57 €	227.000,00 €
	Sistema di encription dati sensibili	32.786,89 €	40.000,00 €
	Registro delle attività di trattamento	16.393,44 €	20.000,00 €
	Sistema di gestione informatizzata dei consensi informati	32.786,89 €	40.000,00 €
	Sistema di registro log Active Directory per copia documenti sensibili, cambio psw	8.606,56 €	10.500,00 €
	NAS per archiviazione dati	8.196,72 €	10.000,00 €
	Sistema di Cyber defence comprensivo di rilevamento delle minacce in tempo reale e loro risoluzione	53.688,52 €	65.500,00 €
	Sistema informatizzato servizio di recall esame paziente comprensivo di pacchetto SMS	9.836,07 €	12.000,00 €
	N.4 sistemi di videoconferenza	8.196,72 €	10.000,00 €
	TOTALE COMPLESSIVO SCHEDA 3	**356.557,38 €**	**435.000,00 €**