Linee di indirizzo per la corretta gestione di cyber attacchi alle Reti e ai Sistemi informativi trasfusionali

Febbraio 2023

CENTRO NAZIONALE SANGUE
Istituto Superiore di Sanità

Linee di indirizzo per la corretta gestione di cyber attacchi alle Reti e ai Sistemi informativi trasfusionali

Elaborato nell'ambito del Gruppo di lavoro "ad hoc" costituito dal Centro Nazionale Sangue

Redatto da:

Giuseppe Bellifemine, Ministero della Salute
Giovanni Camisasca, Regione Piemonte
Ivano Coretti, Centro regionale sangue Emilia Romagna
Massimo La Raja, Azienda sanitaria universitaria Giuliano Isontina (ASUGI)
Samantha Profili, Centro nazionale sangue
Simonetta Pupella, Centro nazionale sangue
Erica Solimbergo, Azienda Ospedale Università Padova
Carlo Villanacci, Istituto Superiore di Sanità

Revisionato da:

Pasquale Colamartino, Tavolo della Sub Area Servizi trasfusionali della Conferenza delle Regioni e PP.AA.
Mauro Dionisio, Ministero della Salute
Stefania Vaglio, Centro regionale sangue Lazio
Vanda Randi, Centro regionale sangue Emilia Romagna.

Rev. 0 – Febbraio 2023

Sommario

Presentazione

La sicurezza e la prevenzione dell'errore umano che ci è consentita grazie ai sistemi informatici è certamente uno dei grandi successi della tecnologia degli ultimi trent'anni. Mai come oggi i grandi gestionali, che ci garantiscono l'accesso a dati verificati e certi, si avvantaggiano di un sistema di connessioni che crea un'enorme rete di cui ci gioviamo nel nostro lavoro quotidiano e che ci consentono di conoscere informazioni sicure e validate, talvolta anche a distanza dal luogo dove si svolge il nostro lavoro, come sta accadendo con le applicazioni della telemedicina. Al contempo, si accresce però la vulnerabilità delle reti informatiche le quali, se non adeguatamente protette, possono essere attaccate da malintenzionati ed essere oggetto di azioni criminose, le cui conseguenze sono note a tutti. Il sistema trasfusionale è particolarmente suscettibile alle conseguenze degli attacchi informatici, come abbiamo visto nel recente passato in diverse situazioni in Italia. Per questa ragione si è sentita la necessità di dare indicazioni e suggerimenti sperabilmente utili nei casi in cui l'intrusione informatica renda inutilizzabile, per tempi più o meno lunghi, i nostri sistemi informatici. Come nel caso di ogni "malattia infettiva" (cui i cyberattacchi somigliano molto, a cominciare dall'intruso che non per nulla chiamiamo "virus"), l'arma principale rimane la prevenzione, molto legata ai corretti comportamenti che gli utenti devono tenere per impedire di lasciare distrattamente aperte "porte" in cui gli intrusi si infilano. Quando però (anche senza dolo o colpa) l'infezione si verifica, bisogna garantire comunque l'operatività basilare delle nostre strutture trasfusionali, per garantire le terapie trasfusionali salvavita, dando tempo agli esperti di intervenire e portare il sistema alla "restitutio ad integrum". Chi avrebbe immaginato, quando abbiamo iniziato ad appoggiarci ai sistemi informatici, che avremmo nel futuro trattato queste reti con lo stesso linguaggio con cui parliamo delle malattie diffusive...

Sono davvero molto grato a tutti gli esperti del gruppo di lavoro e di revisione per il contributo importantissimo che hanno dato alla stesura di queste linee di indirizzo: alcuni sono diventati "esperti" loro malgrado, per avere subito le conseguenze del cyberattacco e quindi il loro contributo è particolarmente prezioso. Mentre mi compiaccio per la pubblicazione di questo documento, mi auguro che non dobbiamo più, nel futuro, affrontare le conseguenze di queste intrusioni; ma se sciaguratamente dovesse capitare, da oggi abbiamo qualche arma in più.

Vincenzo De Angelis
Direttore Centro nazionale sangue

Introduzione

Perché la sicurezza informatica è un problema rilevante per il sistema sanitario e per quello trasfusionale in particolare?

La *cybersecurity* è un elemento percepito e riconosciuto ormai come totalmente trasversale in tutti gli aspetti della vita comunitaria. Negli ultimi anni in Italia il numero di attacchi *cyber*, anche nel settore sanitario, è esponenzialmente aumentato. I sistemi gestionali trasfusionali sono particolarmente a rischio quando sono connessi ai server per mezzo delle reti informatiche aziendali o regionali che, in più di una occasione, si sono dimostrate vulnerabili agli attacchi, in particolare di *malware* "*ransomware*". L'attività produttiva trasfusionale (raccolta, lavorazione, qualificazione), e quindi la disponibilità di emocomponenti, è esposta alla massima criticità laddove, come accaduto nel recente passato, la sospensione dei servizi informatici si prolunga per settimane. Per questi motivi anche per i Servizi Trasfusionali, in collaborazione con i Servizi Informatici aziendali, regionali e centrali, risulta strategico elaborare piani preventivi per impedire una pericolosa disfunzione nell'erogazione delle prestazioni sanitarie essenziali in caso di *cyber attack*.

L'intensificarsi di attacchi alla sicurezza delle Reti informatiche sanitarie, di seguito indicati *cyber* attacchi, impone al sistema sanitario l'esigenza di mettere in atto le misure necessarie a prevenire la perdita e/o la compromissione di dati, di sistemi e finanche dell'intero comparto di Information Technology. Gli impatti di eventuali *cyber* attacchi ad una singola struttura sanitaria o al sistema sanitario regionale possono avere ripercussioni più o meno pesanti anche sui sistemi informativi trasfusionali, mettendo a rischio la sicurezza, l'integrità, la riservatezza dei dati correlati alle attività trasfusionali nonché il regolare svolgimento delle attività stesse.

Scopo

Il presente documento intende, prioritariamente, fornire linee di indirizzo organizzative per preservare la sicurezza delle reti e dei sistemi informativi che supportano la catena trasfusionale nell'evenienza di *cyber* attacchi, nonché per garantire la continuità in sicurezza di quelle funzioni informatiche che supportano l'erogazione della terapia trasfusionale in regime ordinario e nell'emergenza.
In seconda istanza, il documento intende declinare alcuni elementi basilari di conoscenza delle misure generali per la sicurezza informatica, declinate nelle linee guida all'uopo redatte dai competenti Uffici del Ministero della salute, nonché le indicazioni sulle misure di protezione dei dati informatici basate sul comportamento degli operatori, quale contesto di riferimento all'interno del quale si collocano le Reti trasfusionali.

Campo di applicazione

Il presente documento si applica ai sistemi informativi dei servizi trasfusionali sia in relazione ai requisiti minimi delle configurazioni *hardware*, *software* e delle reti collegate, sia in relazione alla gestione dei rischi correlati agli effetti potenziali di un *cyber* attacco e alle conseguenti misure di protezione e di contrasto da adottare.

Lista degli acronimi e delle abbreviazioni

AGID	Agenzia per l'Italia Digitale
BC	Business Continuity
CERT	Computer Emergency Response Team
CISR	Comitato interministeriale per la sicurezza della Repubblica
CSIRT	Computer Security Incident Response Team
DB	Data Base
D.lgs.	Decreto legislativo
DM	Decreto ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DR	Disaster Recovery
ENISA	Agenzia dell'Unione europea per la cibersicurezza
GDPR	General Data Protection Regulation
HL7	Health Level Seven
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ICT	Information and Communications Technology
IHE	Integrated Health Enterprise
KPI	Key Performance Indicator
MFA	Multi Factor Autentication
MPI	Message Passing Interface
NIS	Network and Information Security Directive
OSE	Operatori di Servizi essenziali
OTP	One Time Password
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SGI	Sistema Gestionale Informatizzato
SLA	Service Level Agreement,
ST	Servizio Trasfusionale
UE	Unione Europea
VPN	Virtual Private Network

1. Il contesto normativo europeo e nazionale in ambito di *Cybersecurity*

Quali sono le normative e linee guida di riferimento nella *Cybersecurity?*

La rilevanza del problema della *Cybersecurity* è alla base di alcuni significativi interventi normativi degli ultimi anni, di livello europeo e nazionale. Tra questi ha giocato un ruolo fondamentale la c.d. Direttiva NIS (*Network and Information Security Directive*), adottata dal Parlamento europeo il 6 luglio 2018, sulla sicurezza dei sistemi delle reti e dell'informazione. Di particolare rilevanza è quanto la Direttiva prevede per gli operatori dei servizi essenziali (OSE), tra cui vi sono anche i servizi per la salute, e per i Fornitori di Servizi Digitali. Secondo la direttiva NIS gli OSE devono dotarsi di misure di sicurezza appropriate e di meccanismi di notifica all'autorità nazionale competente in caso di gravi incidenti di sicurezza. Per agevolare e supportare gli OSE del settore salute nell'adempimento dei propri obblighi, l'Autorità NIS del Ministero della salute, in accordo con le Regioni e le Provincie autonome di Trento e Bolzano, ha predisposto apposite linee guida.

La *cybersecurity* è un elemento percepito e riconosciuto come ormai totalmente trasversale in tutti gli aspetti della vita comunitaria. La normativa ha subito negli ultimi anni molteplici sviluppi, sia per restare al passo con le esigenze del mercato sia per garantire un'adeguata protezione dei diversi settori nazionali e dei propri patrimoni informativi. La trasversalità e rilevanza della *cybersecurity* hanno reso necessari mirati interventi normativi da parte della Commissione Europea e delle singole Autorità Nazionali, in termini di direttive, regolamenti, linee guida, gruppi di lavoro e iniziative di settore.

La pandemia COVID ha inoltre contribuito ad accelerare tali interventi, considerando che il numero di attacchi *cyber* negli ultimi due anni, specialmente nel settore sanitario, è esponenzialmente aumentato. In breve tempo è nettamente aumentata la necessità di accedere a sistemi e servizi da remoto, rendendo evidente sia una carenza di consapevolezza da parte degli utenti rispetto ai rischi di sicurezza informatica sia la necessità da parte delle organizzazioni in ambito pubblico e privato di fronteggiare in modo efficace i rischi e le minacce crescenti in tale ambito.

Vengono riportati in Allegato 1 al presente documento gli interventi normativi più significativi degli ultimi anni, a livello europeo e nazionale, nel settore della *cybersecurity*.

Tra questi interventi ha giocato un ruolo fondamentale la c.d. Direttiva NIS (*Network and Information Security Directive*), adottata dal Parlamento europeo il 6 luglio 2018, sulla sicurezza dei sistemi delle reti e dell'informazione. Essa rappresenta il primo insieme di regole sulla sicurezza informatica univoco a livello dell'Unione Europea (UE), al fine di raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri.

Gli elementi più significativi di tale direttiva sono i seguenti:

- migliorare le capacità di *cybersecurity* dei singoli Stati dell'Unione;
- aumentare il livello di cooperazione tra gli Stati dell'Unione;
- efficientare la gestione dei rischi e garantire la comunicazione degli incidenti di rilevante entità da parte degli operatori dei servizi essenziali (OSE) e dei fornitori di servizi digitali.

Per poter migliorare le capacità *cyber*, ogni Stato ha dovuto dotarsi, qualora già non l'avesse, di una strategia nazionale di *cybersecurity* attraverso la definizione di obiettivi strategici, priorità nazionali, *governance*, misure proattive, risposta e *recovery*; sensibilizzazione, formazione ed istruzione; incentivazione della cooperazione tra settore pubblico e settore privato; attori coinvolti nella attuazione della strategia.

Inoltre, la direttiva NIS richiede agli Stati di designare una o più Autorità competenti per il controllo dell'applicazione della direttiva stessa a livello nazionale. Un singolo punto di contatto deve essere designato da ognuno degli Stati membri, con il compito di assicurare la cooperazione internazionale e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati nella direttiva stessa.[1] Ogni Stato è inoltre tenuto a designare uno o più *Computer Security Incident Response Team* (CSIRT) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti; gli stessi CSIRT sono tenuti a fornire analisi sui rischi e incidenti al fine di aumentare il grado di consapevolezza in tale ambito.

Infine, particolare rilevanza assume quanto previsto per gli OSE e i fornitori di servizi digitali. Gli OSE sono aziende pubbliche o private che hanno un ruolo importante per la società e l'economia e che devono dotarsi di misure di sicurezza appropriate e di meccanismi di notifica all'autorità nazionale competente in caso di gravi incidenti di sicurezza (secondo parametri legati al numero di utenti coinvolti, durata dell'incidente e diffusione geografica).

Gli OSE vengono identificati direttamente da ogni Stato membro nei settori energia, trasporti, banche e società finanziarie, salute, acqua ed infrastrutture digitali. I criteri per l'individuazione degli enti inclusi in questa lista sono i seguenti:

- essenzialità del servizio offerto per il mantenimento di attività critiche in ambito economico e sociale;
- dipendenza del servizio da sistemi informatici;
- effetti gravi e significativi dell'incidente di sicurezza sulla fornitura di un servizio essenziale.

Anche i fornitori di servizi digitali sono tenuti, secondo la direttiva NIS, ad attuare misure di sicurezza appropriate e a notificare incidenti rilevanti. Oltre alle misure già previste per gli operatori di servizi essenziali, le misure di sicurezza relative ai fornitori di servizi digitali prevedono alcuni fattori specifici, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali. Tra i fornitori di servizi digitali sono inclusi anche i mercati *on-line*, i servizi *cloud* ed i motori di ricerca. Non rientrano in questa categoria invece le piccole e medie imprese.

a. Le linee guida per gli operatori dei servizi essenziali – settore salute

Per agevolare e supportare gli OSE del settore salute nell'adempimento dei propri obblighi, l'Autorità NIS del Ministero della salute, in accordo con le Regioni e le Provincie autonome di Trento e Bolzano, ha predisposto apposite linee guida.

Le Linee guida per gli OSE costituiscono uno strumento operativo di supporto al processo di gestione e trattamento del rischio *cyber*, per affrontare in modo organico e qualificato la gestione della sicurezza delle reti e dei sistemi informativi.

A tale scopo le linee guida sono basate sul "*Framework Nazionale per la Cyber Security e la Data Protection*", un riferimento da poter considerare assoluto per le misure di sicurezza, gli standard e le norme di settore (vedi Allegato 1) secondo un principio di neutralità tecnologica, che non va ad imporre agli operatori l'impiego di specifiche soluzioni di *Information and Communications Technology* (ICT), bensì suggerisce un approccio razionale e dinamico strettamente connesso all'analisi del rischio.

[1] Cfr. Laboratorio Nazionale di Cyber Security (2015), Il Futuro della Cyber Security in Italia, Consorzio Interuniversitario Nazionale per l'Informatica

Le citate linee guida disciplinano inoltre le procedure di notifica obbligatoria degli incidenti rilevanti sulla continuità dei servizi essenziali forniti e inoltre mirano a promuovere azioni concrete di prevenzione attraverso meccanismi di "*early warning*" che fanno uso del sistema delle notifiche anche volontarie per la condivisione delle informazioni sugli incidenti con la comunità di sicurezza nazionale posta a protezione dello spazio cibernetico.

b. Framework nazionale per la cybersecurity

Il Framework Nazionale per la Cybersecurity e la Data Protection rappresenta un consolidato standard preso come riferimento da soggetti fortemente eterogenei (dalla Pubblica Amministrazione alla piccola impresa) e adottato come strumento per l'organizzazione della propria strategia di difesa rispetto alle minacce cibernetiche. Le norme citate nel presente documento, che in diversi settori hanno imposto vincoli legati alla gestione della sicurezza dei sistemi ICT, hanno ulteriormente evidenziato quanto sia necessaria l'adozione di un *framework* di *cybersecurity*: qualsiasi organizzazione dovrà valutare quanto le misure di sicurezza implementate permettano di soddisfare i requisiti stabiliti dall'obiettivo finale, in base a un percorso volto all'incremento del livello di sicurezza.

Il citato *framework* eredita le tre nozioni fondamentali del *Cybersecurity Framework del National Institute of Standards and Technology*: *Framework Core*, *Profile* e *Implementation Tier*.

Framework Core – Il *core* rappresenta la struttura del ciclo di vita del processo di gestione della *cybersecurity*, sia dal punto di vista tecnico sia organizzativo. Il *core* è strutturato gerarchicamente in funzioni (*functions*), categorie (*categories*) e sotto categorie (*sub-categories*). Le funzioni, concorrenti e continue, sono: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico. Il *Framework* quindi definisce, per ogni funzione, categoria e sottocategoria, le attività abilitanti e quali processi e tecnologie mettere in campo per gestire la singola funzione. Il *Framework Core* presenta inoltre delle *informative reference*, vale e dire dei riferimenti che legano la singola sottocategoria alle pratiche di sicurezza note previste da standard di settore (ISO, SP800-53r4, COBIT-5, SANS20 e altri) o da regolamentazioni generali vigenti (Regolamento UE 2016/679 *General Data Protection Regulation - GDPR*, Direttiva UE 2016/1148 NIS).

La struttura del *Framework Core* è riportata nella seguente Figura 1.

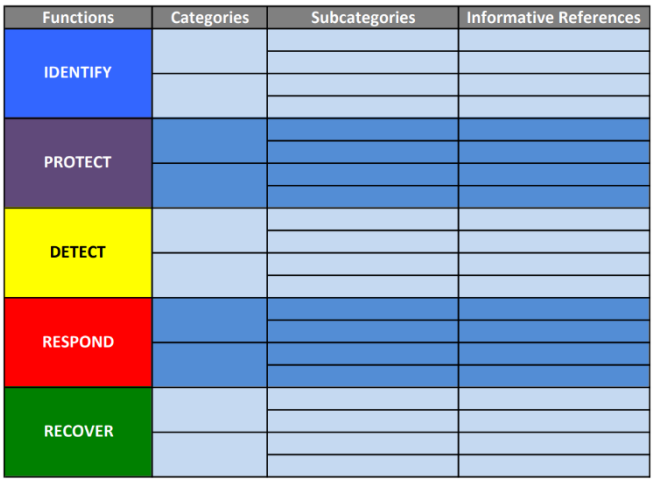

Figura 1- Functions del Framework Nazionale

Di seguito è riportata una breve descrizione delle 5 funzioni del *Framework Core*.

IDENTIFY – La function IDENTIFY è legata alla comprensione del contesto aziendale, degli *asset* che supportano i processi critici di *business* e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le *category* all'interno di questa function sono: *Asset Management*, *Business Environment*; *Governance*, *Risk Assessment*, *Risk Management Strategy*, *Supply Chain Risk Management* e *Data Management*.

PROTECT – La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le *category* all'interno di questa function sono: *Identity Management*, *Authentication and Access Control*, *Awareness and Training*, *Data Security*, *Information Protection Processes and Procedures*, *Maintenance,* Protective Technology.

DETECT – La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le *category* all'interno di questa *function* sono: *Anomalies and Events, Security Continuous Monitoring*, *Detection Processes*.

RESPOND – La *function* RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le *category* all'interno di questa function sono: *Response Planning*, *Communications*, *Analysis*, *Mitigation*, *Improvements*.

RECOVER – La *function* RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle *business operations*. Le categorie all'interno di questa funzione sono: *Recovery Planning*, *Improvements*, *Communications*.

Il *Framework* inoltre incorpora nel *core* nuove categorie e sottocategorie riguardanti la protezione dei dati personali non presenti nelle prime versioni.

2. I sistemi informativi dei servizi trasfusionali – analisi del contesto e linee di sviluppo

Quali sono i requisiti per garantire la sicurezza dei sistemi informatici e la loro operatività anche in caso di attacco informatico?

La prevenzione degli attacchi informatici e la minimizzazione dei danni e delle interruzioni dei sistemi informatici può essere garantita da una specifica qualifica dei *software*, dei server, delle modalità di *storage* e delle reti di interconnessioni tra sistemi. Queste qualifiche devono fare riferimento alle linee guida AGID e l'installazione del Sistema informativo dovrebbe essere prevista in *cloud (IaaS)* su soluzioni di *Web Farm* con certificazioni ISO applicabili. Per la soluzione infrastrutturale sono auspicabili qualificazioni come CSP (Cloud Service Provider), accreditamento AGID con infrastrutture riconosciute dalla stessa come candidabili ad essere utilizzate dal Polo Strategico Nazionale; inoltre, se disponibile, certificazione in base alla *Tier Certification* dell'*Uptime Institute* quale data *Center Tier III* o in base allo standard ANSI TIA 942 quale *Rated-3*.
In estrema sintesi, la componente fisica architetturale deve essere disegnata al fine di raggiungere i seguenti obiettivi strategici:

- sicurezza fisica e logica dei dati;
- elevate prestazioni;
- garanzia di continuità operativa sul Sito di Produzione (BC mediante server ridondati);
- *backup* operativo;
- realizzazione di un'architettura di DR con duplicazione su un data center geograficamente distinto;
- minimizzazione del tempo di ripristino sul sito di DR;
- qualità e certificazione delle componenti;
- garantire l'integrità, la ridondanza, la continuità, la disponibilità e la riservatezza dei sistemi informativi gestiti;
- connessioni sicure (ad es.: VPN) per realtà non aziendali che devono connettersi al sistema (vedi punti di raccolta associativa).

I sistemi informativi dei Servizi Trasfusionali (ST) sono, nella maggioranza dei casi, basati su una architettura fisica di tipo *client-server*, che si è mostrata vulnerabile agli attacchi informatici, come dimostrano alcune recenti esperienze in Regione Lazio e Regione Veneto. In considerazione del fatto che i sistemi informativi dei ST supportano l'erogazione di prestazioni assistenziali ricomprese nei livelli essenziali di assistenza (LEA), si rende necessario pianificare interventi di rafforzamento delle attuali architetture informatiche, sia in termini di *hardware* sia di software per prevenire e rispondere agli attacchi e garantire la continuità assistenziale.

La progettualità e la realizzazione dei sistemi snformativi dei ST deve tener conto dell'evoluzione tecnologica a livello *hardware* e *software*, volta a garantire la *cyber security* e la *safety*. I moderni sistemi informativi dei ST dovrebbero essere *software web-based* che, attraverso protocolli e paradigmi di comunicazione standard (ad es.: HL7, IHE, ecc.), gestiscano i processi dei ST e garantiscaono sia gli interfacciamenti con gli strumenti sia le integrazioni con gli applicativi aziendali.

Le moderne componenti applicative dovrebbero essere progettate e realizzate in modo tale da consentire la standardizzazione dei processi e, al tempo stesso, la massima configurabilità di oggetti e procedure operative che nel tempo potrebbero variare (ad es.: ambito normativo) o che

contraddistinguono specifiche realtà aziendali, sovra-aziendali (Aree Vaste, Aree Metropolitane, ecc.) e/o regionali.

I moduli applicativi dovrebbero essere realizzati basandosi su un'architettura *Model view controller* così da separare fisicamente la logica di *front-end* dalla logica di *business*, in aderenza al paradigma *Rich Internet Application*.

a. Configurazione dei sistemi (hardware, software, reti)

L'accesso a tali sistemi informativi deve avvenire attraverso l'identificazione dell'utente. Questo può realizzarsi mediante differenti meccanismi di autenticazione:

- ID personale e *password*;
- mediante interscambio di certificati tra *client* e *server*;
- OTP – *One Time Password*.

Oggigiorno, tali logiche sono superate da concetti di identificazione centralizzata che garantiscono una maggiore sicurezza. Questo si realizza mediante l'integrazione dei sistemi informativi con sistemi esterni, quali:

- *Sistemi di Autenticazione federate regionali (SAML2)*: è un sistema di *single sign-on* (SSO) per reti informatiche che consente di autenticarsi su sistemi differenti, permettendo di effettuare il login su reti di organizzazioni o istituzioni diverse, utilizzando una sola identità.
- *SPID (Sistema Pubblico di Identità Digitale)*: medesimo sistema per utenti non appartenenti all'azienda che accedono quindi dall'esterno (ad es.: associazioni di volontariato, donatori, ecc.).

Qualunque sia il meccanismo di autenticazione all'applicativo, è importante che l'accesso ai sistemi avvenga in modalità Multi Factor Autentication (MFA), con un doppio fattore di autenticazione (es. OTP), che la *password* abbia una complessità uguale o superiore a quanto richiesto dall'art. 32 del GDPR, ovvero sia adeguata in relazione al sistema che deve proteggere. La necessità di integrazione e standardizzazione dell'infrastruttura tecnologica e la complessità del contesto operativo dei ST, legato all'elevata numerosità delle sedi, all'ampiezza del territorio ed alle articolate realtà organizzative, si devono tradurre in ponderate scelte a livello di infrastruttura *hardware*, *software* nonché di rete. La componente fisica architetturale deve essere disegnata al fine di raggiungere i seguenti obiettivi strategici:

- sicurezza fisica e logica dei dati;
- elevate prestazioni;
- garanzia di continuità operativa sul Sito di Produzione e su un secondo sito geograficamente distinto anche se vicino (*business continuity* mediante *server* ridondati);
- *backup* operativo;
- realizzazione di un'architettura di DR con duplicazione su un *data center* geograficamente distinto e più lontano dai due siti di produzione;
- minimizzazione del tempo di ripristino sul sito di DR;
- qualità e certificazione delle componenti;
- gestione dell'integrità, della ridondanza, della continuità, della disponibilità e della riservatezza dei sistemi informativi gestiti;
- connessioni sicure ad es.: *Virtual Private Network* – VPN) per realtà non aziendali che devono connettersi al sistema (vedi punti di raccolta associativi).

L'architettura *hardware* deve prevedere l'implementazione di un sito di produzione, in modo da coprire l'esigenza di resilienza intra-sito, grazie a ridondanze e protezioni *hardware*, e relativo sito di DR, tale da garantire la protezione da eventuale indisponibilità fisica a medio termine del sito di produzione. I siti

preferibilmente devono essere implementati utilizzando gli stessi apparati *hardware*, configurati specularmente in modo da semplificare la gestione e velocizzare eventuali operazioni di ripristino in DR.

Storage

La dotazione *storage* su entrambi i siti deve essere contraddistinta da soluzioni flessibili, espandibili, con elevate *performances*, affidabili e caratterizate da un sistema di replica e ridondanza. La capacità deve essere dimensionata alla realtà specifica (sistemi, *data base*, *cache* e *backup*). Devono essere messi in atto efficienti sistemi per la protezione sia dello *storage* che del dato.

Business Continuity

La *business continuity* (BC) può essere assimilata a uno "*0 downtime*" sull'infrastruttura tecnologica e si riferisce alla possibilità di progettare l'architettura, attraverso un sistema in *cluster*, in modo da garantire una continua operatività della stessa in caso di grave danno ad uno o più componenti del sistema. A differenza del DR, un piano di BC prevede che, durante il verificarsi di malfunzionamenti, i sistemi continuino ad essere attivi e funzionanti, senza interruzioni.

Per realizzare questo obiettivo, è necessario mettere a punto un progetto in cui i dati siano sincronizzati nel medesimo *data center* o su due *data center* diversi (geograficamente vicini) grazie a strategie lato *hardware* e *software*. Generalmente, l'utente che utilizza l'applicativo su un sistema di BC, in caso di guasto, sperimenterà solo una breve pausa ma senza accorgersi che si sia verificato un problema. A livello applicativo, deve essere gestita automaticamente anche l'indisponibilità di uno dei server DB.

Conditio sine qua non della BC è la distribuzione dei servizi ICT su uno o più *data center* che però non distino tra loro oltre 20 km. Infatti, maggiore è la distanza maggiori saranno anche i tempi di *recovery*. In particolare, tra 5 e 50 km, aumentando la distanza si riduce il rischio ma si rallentano progressivamente le prestazioni delle transazioni da eseguire in BC.

Caratteristiche di un piano di BC sono:

- la pianificazione delle attività volte a garantire la continuità lavorativa senza interruzioni (ordine del minuto) al verificarsi di malfunzionamento di una o più componenti;
- l'analisi preliminare dei rischi;
- la collocazione dei *server* su uno o più *data center* geograficamente vicini al fine di non incidere troppo sulle prestazioni.

Per ulteriori approfondimenti fare riferimento alle "Linee Guida per il *Disaster Recovery* delle Pubbliche Amministrazioni" ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale.

Disaster Recovery

Adottare una politica di DR vuol dire avere un sito secondario in cui salvare tutti i dati e gli *application server*, potendo quindi rendere nuovamente disponibile il servizio in caso di catastrofi naturali (incendi, uragani, terremoti o qualsiasi evento accidentale o doloso possa mettere a rischio la funzionalità di un *data center*). Da notare che, in caso di effettivo disastro, il ripristino del servizio non è automatico e richiede un intervento tecnico e la velocità del ripristino dipende dal modello di infrastruttura adottato e dai processi che ne sono alla base e che saranno stati preventivamente testati.

Nella realizzazione di un piano di DR bisogna tener conto di:

- *recovery time objective* (RTO) ossia la durata massima del fermo, che va stabilita al momento della pianificazione: in tal modo l'azienda sa già in anticipo a quanto tempo di disagio va incontro avendo progettato la DR in modo da tollerare una certa durata massima di *downtime*.

- recovery point objective (RPO) che stabilisce invece la quantità massima di dati a cui un'azienda è disposta a rinunciare a seguito di un disastro.

Anche se l'RPO si riferisce a una quantità di dati si misura in unità di tempo, come l'RTO, quindi l'ammontare dei dati persi dipende da quanti se ne producono per unità di tempo. Oltre che stabilire durante il progetto RTO ed RPO è necessario, al fine di realizzare un DR geografico, dislocare i servizi ICT in nodi geograficamente distribuiti con una certa distanza l'uno dall'altra. La distanza minima del sito secondario non è stabilita in maniera netta e più che delle regole esistono delle *best practice*. Una *best practice* di DR prevede tra i 50 ed i 100 km di distanza per repliche asincrone (bassi RPO), oltre i 100km di distanza per repliche asincrone (RPO più alti).

Caratteristiche di un piano di DR sono:

- l'analisi dei rischi preliminare;
- la pianificazione delle attività da mettere in atto in caso di disastro (ad es.: malfunzionamento/rottura del sito di produzione);
- la valutazione di RTO e RPO ossia, rispettivamente, l'obiettivo temporale di recupero del *business* e la massima finestra temporale entro la quale il sistema deve essere riattivato;
- l'analisi dei costi (direttamente proporzionali a quanto saranno ambiziosi RTO e RPO);
- la collocazione dei *server* su due o più *data center* distanti geograficamente a una distanza in km ragionevolmente elevata;
- la definizione della politica di backup dei dati del Sito di Produzione, sia in modalità "sincrona" sia *offline*, ovvero salvata su un mezzo esterno scollegato al *server* operativo una volta completata la copia di sicurezza dei dati, in caso di *crypto ransomware* (*malware* in grado di criptografare i dati rendendoli inutilizzabili).

Per ulteriori approfondimenti fare riferimento alle "Linee Guida per il *Disaster Recovery* delle Pubbliche Amministrazioni" ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale.

Gestione interfacciamenti strumentali

La gestione degli interfacciamenti con gli strumenti deve essere gestita esclusivamente attraverso standard consolidati, quail HTTPS, *web services*, HL7, XML, ecc. Deve essere disponibile:

- un *sinottico*, aggiornato in *real time*, in grado di rappresentare graficamente lo stato di collegamento degli strumenti del ST, così da individuare in modo rapido ed intuitivo eventuali anomalie di funzionamento;
- un *device* che implementa il protocollo di comunicazione definito dal produttore degli strumenti, in accordo con i servizi competenti delle Aziende coinvolte, per la ricezione delle liste di lavoro dal sistema informativo (solo se la modalità di comunicazione è bidirezionale) e per l'invio dei dati/risultati dagli strumenti. Ogni singola Azienda coinvolta avrà un proprio *device*: il *device* è l'unico che comunica con gli strumenti. I *devices* devono essere in grado di funzionare anche in caso di assenza momentanea della connessione al sistema informativo dei ST, in modalità *offline*, e di sincronizzarsi successivamente con gli strumenti per recuperare i dati;
- un *middleware, che* rappresenta lo strato intermedio posizionato tra i *devices* ed il sistema informativo dei ST, ovvero i *devices* comunicano unicamente con il *middleware*. Tutte le comunicazioni sono effettuate tramite protocollo HTTPS.

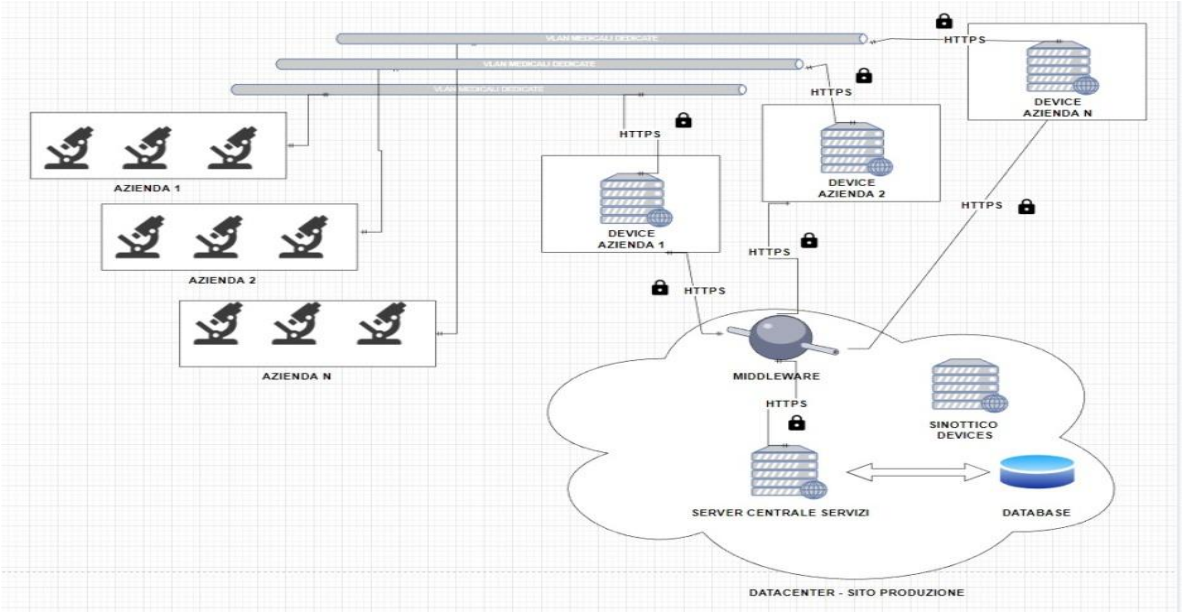

Figura 2- Sinottico degli interfacciamenti strumentali

Gestione integrazioni applicative

Il sistema informativo deve integrarsi con il Sistema Informativo Ospedaliero (SIO) delle diverse Aziende coinvolte secondo paradigmi di comunicazione standard (ad es.: HL7, IHE, ecc.). A titolo esemplificativo, ma non esaustivo, le principali integrazioni applicative sono:

- Anagrafica Centralizzata / MPI aziendale;
- LIS (Laboratory Informative System);
- CUP (Centro Unico Prenotazione);
- ADT (Ammissione, Dimissione, Trasferimento);
- CCE (Cartella Clinica Elettronica);
- *Order Entry*;
- *Repository*;
- Trasfusione sicura.

Monitoraggio

È possibile usare il monitoraggio per ottenere informazioni dettagliate sulla correttezza del funzionamento di un sistema prevedendo apposite *service control rooms*. Il monitoraggio è una parte fondamentale della gestione degli obiettivi di qualità del servizio e riguarda i seguenti aspetti.

- Garanzia dell'integrità del sistema tramite sistema a semafori che tenga conto di:
    - frequenza delle richieste dirette a ogni servizio o sottosistema,
    - tempi di risposta di tali richieste,
    - volume del flusso dei dati in entrata e in uscita da ogni servizio.

  I dati a supporto del monitoraggio dello stato sono:
    - esecuzione delle richieste degli utenti;
    - monitoraggio sintetico degli utenti;
    - eccezioni di registrazione, errori e avvisi;

- monitoraggio dell'integrità di eventuali servizi di terze parti usati dal sistema;
- monitoraggio *endpoint*;
- monitoraggio componenti infrastrutturali (ad es.: utilizzo della CPU in *background*, utilizzo della memoria, numero di *thread*, tempo di elaborazione della CPU, lunghezza della coda di richieste, velocità ed errori di I/O del disco o della rete, numero di byte scritti o letti, indicatori di *middleware*).

- Tracciabilità della disponibilità del sistema e dei relativi componenti al fine di generare statistiche riguardanti il tempo di attività del sistema stesso.
  I dati necessari per tener traccia della disponibilità potrebbero dipendere da diversi fattori di basso livello, molti dei quali potrebbero essere specifici dell'applicazione, del sistema e dell'ambiente. Un sistema di monitoraggio efficace, mediante registrazione delle eccezioni, degli errori e degli avvisi che potrebbero verificarsi, acquisisce i dati di disponibilità che corrispondono a questi fattori di basso livello e quindi vengono aggregati in modo da offrire una panoramica del sistema. Deve anche essere in grado di avvisare rapidamente il gestore dell'applicativo quando uno o più servizi non funzionano o quando gli utenti non riescono a connettersi ai servizi, così come può essere utile consentire al sistema di generare un avviso relativo al numero di errori di connessione a un sottosistema specifico durante un determinato periodo di tempo. Tutti i *timeout,* gli errori di connettività di rete e i tentativi di connessione devono essere registrati. Tutti i dati devono riportare un *timestamp* e vanno calcolati e registrati i *downtime* del sistema o delle sue componenti.

- Gestione delle *performances*: le prestazioni del sistema dipendono da numerosi fattori, ogni fattore in genere viene misurato tramite KPI - *Key Performance Indicator* (ad es.: il numero di transazioni di DB al secondo o il volume di richieste di rete gestite correttamente nell'intervallo di tempo specificato). Bisogna inoltre monitorare:
  - velocità di risposta per le richieste degli utenti,
  - il numero di richieste utente simultanee,
  - il volume di traffico di rete,
  - la velocità a cui le transazioni aziendali vengono completate,
  - il tempo medio di elaborazione delle richieste,
  - il numero di utenti simultanei rispetto al tempo di latenza della richiesta, ovvero il tempo che trascorre tra l'invio di una richiesta da parte di un utente e l'inizio dell'elaborazione della richiesta stessa,
  - il numero di utenti simultanei rispetto al tempo medio di risposta, ovvero il tempo necessario per il completamento di una richiesta dall'avvio dell'elaborazione,
  - il volume di richieste rispetto al numero di errori di elaborazione.
- Garanzia dei contratti di servizio (SLA) definiti con il cliente. I contratti di servizio vengono spesso definiti in termini di:
  - disponibilità complessiva del sistema (ad es. per sistemi critici come il sistema informativo dei ST si tende al 99,99% del tempo);
  - velocità effettiva operativa (ad es. sistema in grado di supportare fino a 100.000 richieste utente simultanee);
  - tempo di risposta operativa (ad es. garanzie in relazione alla velocità di elaborazione delle richieste);
  - definizione di apposite penali in caso di violazione dei termini stabiliti nel contratto di servizio.

- Protezione della privacy e sicurezza del sistema e dei relativi dati. La complessità del meccanismo di sicurezza è in genere una funzione della riservatezza dei dati. In un sistema che richiede l'autenticazione degli utenti è necessario registrare:
    - tutti i tentativi di accesso, sia quelli con esito positivo sia quelli con esito negativo,
    - tutte le registrazioni e per quelle necessarie anche le visualizzazioni effettuate da un utente autenticato, con i dettagli relativi a tutte le risorse usate,
    - data e ora in cui l'utente ha terminato una sessione e si è disconnesso.

  Il sito di Produzione deve prevedere apposite soluzioni atte a individuare e bloccare eventuali attacchi (es. anti-DDoS, IPS/IDS, WAF e firewalling, VA scanning, ecc..). Il monitoraggio può consentire di rilevare attacchi al sistema. In particolare:
    - rilevare tentativi di intrusione di entità non autenticate,
    - identificare i tentativi di esecuzione di operazioni su dati da parte di entità non autorizzate ad accedere a tali dati,
    - determinare se il sistema o una parte di questo è sotto attacco dall'esterno o dall'interno.

  Per supportare tali requisiti, è necessario che il monitoraggio riceva una notifica se:
    - un account esegue una serie di tentativi di accesso non riusciti entro un periodo specificato, un account autenticato tenta ripetutamente di accedere a una risorsa non autorizzata durante un periodo specificato;
    - si verifica un numero elevato di richieste non autenticate o non autorizzate durante un periodo specificato includendo l'indirizzo dell'*host* di origine di ogni richiesta.

- Tracciabilità delle operazioni eseguite a scopo di controllo o a fini normativi. Il Sito di Produzione deve prevedere soluzioni integrate di Log Management e SIEM. La normativa vigente in materia trasfusionale impone la tracciabilità di tutte le attività effettuate dai clinici nonché la tracciabilità di eventuali modifiche apportate ai risultati. Pertanto il sistema informativo deve essere in grado di tracciare la sequenza delle operazioni eseguite dagli utenti in un certo intervallo temporale mediante sistema di sicurezza per autenticazione utente, *log* di traccia e *log* di sicurezza. L'accesso a tale *repository* deve essere protetto per impedirne la manomissione.

- Monitoraggio sull'utilizzo quotidiano del sistema ed analisi predittiva di eventuali problematiche serve a rilevare l'utilizzo delle funzionalità e dei componenti di un'applicazione al fine di:
    - determinare quali funzionalità siano utilizzate di frequente e determinare le potenziali aree sensibili nel sistema. Gli elementi a traffico elevato potrebbero trarre vantaggio dal partizionamento funzionale o persino dalla replica per distribuire il carico in modo più uniforme e, al tempo stesso, per individuare le funzionalità usate raramente così da valutarne il ritiro o la sostituzione in una versione futura del sistema;
    - ottenere informazioni sugli eventi operativi del sistema durante il normale utilizzo;
    - rilevare l'ora di inizio e fine di ogni richiesta e la natura della richiesta stessa, ovvero di lettura e di scrittura.

  Per esaminare l'utilizzo del sistema, vengono visualizzate le informazioni relative a:
    - numero di richieste elaborate per ogni sottosistema e dirette a ogni risorsa;
    - lavoro eseguito da ogni utente;
    - volume dell'archivio dati occupato da ogni utente;
    - risorse a cui ogni utente accede.

- Operazioni di rilevamento e *debug* di versioni del software: a seguito di un *bug* dell'applicativo, individuate da un utente, è necessario avviare un'analisi della causa radice. Per la traccia di eventi imprevisti e di altri problemi, è fondamentale che i dati di monitoraggio forniscano informazioni sufficienti a consentire ad un analista di risalire all'origine dei problemi e ricostruire la sequenza degli eventi. Individuato il problema, uno sviluppatore provvede ad apportare le modifiche necessarie per la risoluzione del *bug* segnalato / riscontrato.

b. *Controllo dei cambiamenti*

I sistemi informativi dei ST devono essere convalidati secondo GAMP5 (*Good Automated Manufacturing Practices*) sia a livello *hardware* sia *software* e rispondere ai requisiti minimi di funzionalità e sicurezza che i *software* devono soddisfare in relazione all'uso previsto (vedi Allegato XII del Decreto ministeriale 2 novembre 2015[2]).
Deve essere redatto un *Project Validation Plan* nel quale vanno definite la strategia e le attività necessarie per la convalida del sistema informativo dei ST, ovvero:

- la valutazione della criticità e complessità del sistema attraverso l'analisi dei rischi,
- la definizione della strategia di convalida del sistema, i criteri di accettazione di base e le tempistiche di massima,
- l'identificazione della documentazione che deve essere prodotta relativamente ad ogni attività,
- *deliverables* per la validazione ed *user requirements specification* che il sistema informativo deve soddisfare,
- l'identificazione del team di convalida e le responsabilità per il completamento di ogni compito.

Qualora vi siano cambiamenti impattanti su funzionalità e sicurezza del sistema (ad es.: rilascio nuova *release*, non *debugging*) sarà necessario attuare una riconvalida del sistema informativo.
A livello di infrastruttura *hardware* e *software*, il fornitore deve essere in grado di gestire l'intero processo di installazione, configurazione, test, avvio, *tuning*, manutenzione, monitoraggio e aggiornamento. Il servizio di manutenzione deve includere l'aggiornamento di tutti i *software* alle versioni più recenti disponibili sul mercato.
La gestione sistemistica del RDBMS (*Relational Data Base Management System*) è in carico al fornitore dell'applicativo, che potrà accedere da remoto per le attività manutentive periodiche. Il fornitore deve gestire la banca dati e ogni altra componente applicativa al fine di scongiurare degradi di prestazioni nel tempo. In ogni caso i degradi di prestazione non potranno superare un 5% dei valori nominali di prestazioni misurate all'atto del collaudo iniziale di accettazione.
Al fine di garantire la corretta postura di sicurezza informatica con l'introduzione del sistema informativo dei ST, il fornitore deve garantire che quanto oggetto di fornitura è esente da vulnerabilità note mediante produzione di apposita relazione dei controlli effettuati sulla versione installata.
Il fornitore inoltre deve garantire l'aggiornamento tecnologico di quanto oggetto di fornitura in maniera tale da non pregiudicare l'aggiornamento di sicurezza dei *server* e delle infrastrutture fornite a supporto dell'applicativo.
Prima della messa in produzione, tuttavia, ogni aggiornamento e/o nuova *release* deve essere preventivamente concordato, autorizzato, verificato, e validato.

[2] Decreto del ministro della salute n. 69 del 2 novembre 2015 recante "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti".

c. Sistemi di backup

Le soluzioni tecnologiche per il *backup* devono poter disaccoppiare gli ambienti operativi, al fine di evitare che un attacco *ransomware* sull'esercizio possa cifrare anche l'ambiente di *backup* dei dati. Il sistema di *backup* dei dati è la prima forma di protezione per garantire la loro conservazione nel tempo. Per poter rendere agevole la gestione dei *backup*, è necessario organizzare le informazioni opportunamente ed evitare inutili ridondanze del dato nelle diverse tabelle del DB.

Il *backup*, in ottemperanza alle *policies* aziendali, sovraziendali e/o regionali, può essere:

- giornaliero incrementale del DB,
- settimanale completo del DB,
- mensile integrale dei sistemi,
- a seguito di rilascio nuova versione dell'applicativo.

I backup periodici del DB, ci permettono di recuperare i dati a seguito di malfunzionamenti ed errori, quail quelli di:

- funzionamento dei supporti,
- utenti (ad es.: eliminazione di una tabella),
- hardware (ad es.: unità disco danneggiata),
- calamità naturali o altre emergenze gravi.

Un sistema affidabile di *backup* e ripristino richiede pertanto una strategia in grado di bilanciare i requisiti aziendali per la massima disponibilità di dati e la minima perdita di dati, tenendo in considerazione il costo della gestione e dell'archiviazione dei *backup*. Tale strategia prevede una parte relativa al *backup* e una parte relativa al ripristino.
La parte della strategia relativa al *backup* definisce il tipo e la frequenza delle operazioni dello stesso, il tipo e la velocità dell'*hardware* necessario, le modalità di esecuzione di test dei *backup* nonché i percorsi e le modalità di archiviazione dei relativi supporti, incluse le considerazioni relative alla sicurezza.
La parte della strategia relativa al ripristino definisce il responsabile dell'esecuzione delle operazioni di ripristino, la modalità di esecuzione di tali operazioni in modo da realizzare gli obiettivi relativi alla disponibilità del DB e ridurre al minimo il rischio di perdita dei dati e il modo in cui condurre i test sui ripristini.
La progettazione di una strategia di *backup* e ripristino efficace richiede operazioni accurate di pianificazione, implementazione e *testing*. L'esecuzione di test è obbligatoria: una strategia di *backup* può essere considerata efficace solo dopo il completamento del ripristino dei *backup* in tutte le combinazioni incluse nella strategia e l'esecuzione dei test sul DB ripristinato per verificarne la coerenza fisica. È necessario considerare una vasta gamma di fattori, inclusi i seguenti:

- obiettivi relativi al DB di produzione, specie i requisiti relativi alla disponibilità e alla protezione dalla perdita o dal danneggiamento dei dati;
- caratteristiche del DB, ovvero dimensioni, tipo di utilizzo, tipo di contenuto, requisiti relativi ai dati, ecc.;
- vincoli relativi alle risorse (ad es.: *hardware*, personale, spazio per l'archiviazione dei supporti di *backup*, sicurezza fisica dei supporti archiviati, ecc.).

Dopo aver selezionato un modello di recupero che soddisfa le esigenze aziendali o sovraziendali per un determinato DB, è necessario pianificare ed implementare una strategia di *backup* corrispondente. La strategia ottimale dipende da una serie di fattori, i più significativi di seguito riportati:

- numero di ore giornaliere per cui è necessario garantire l'accesso delle applicazioni al DB. (ad es.: è consigliabile pianificare i backup del DB durante le ore notturne);

- frequenza prevista per l'esecuzione di modifiche e aggiornamenti (se le modifiche sono frequenti è consigliabile pianificare *backup* differenziali nei periodi intermedi tra i backup completi del DB così da consentire di ridurre i tempi di ripristino limitando il numero di *backup* del log da ripristinare in seguito al ripristino dei dati);
- ambito previsto per le modifiche, ovvero solo in parti ridotte del DB o in gran parte del DB;
- quantità di spazio su disco necessaria per i *backup*;
- tempi di conservazione dei *backup* del DB.

Assicurarsi di aver definito una pianificazione accurata dei *backup* in base alle esigenze dell'applicazione e ai requisiti aziendali e/o sovraziendali. Man mano che i *backup* diventano datati, il rischio di perdere i dati aumenta a meno che non esista un sistema per rigenerare tutti i dati fino al punto di errore. Prima di scegliere di eliminare i vecchi *backup* a causa di limitazioni delle risorse, considerare se la recuperabilità deve risalire così lontano nel tempo.
Infine è necessario documentare le procedure di *backup* e ripristino e mantenerne una copia nella documentazione relativa alle procedure operative aziendali e/o sovraziendali e mantenere un manuale operativo per ogni DB, in cui indicare la posizione dei *backup*, i nomi dei dispositivi di *backup* (se presenti) e il tempo necessario per il ripristino di quelli di prova.

3. Il processo di gestione dei rischi

Cosa fare nel caso i sistemi informatici non siano utilizzabili per periodi che superano la disponibilità di emocomponenti labili già qualificati?

L'esperienza di alcuni Servizi trasfusionali italiani afferenti a reti aziendali o regionali, vittime di *cyberattack* con blocco prolungato della rete informatica, ha imposto di elaborare, spesso in condizioni di urgenza, un "*disaster plan*" basato sull'analisi dei rischi che prevedesse procedure e soluzioni alternative e che potesse consentire una operatività essenziale del sistema trasfusionale "da vena a vena".
A seconda dei contesti e delle risorse tecnologiche esistenti, sono state allestite diverse opzioni, quali:

- l'elaborazione di un sistema di registrazioni manuali che garantissero in maniera controllata la sicurezza e tracciabilità dei passaggi critici;
- l'utilizzo di un backup di etichette con barcode e di altra documentazione prestampata;
- l'utilizzo di alcune funzioni informatiche mediante PC o strumenti in modalità *offline*;
- l'utilizzo di *hardware* portatili non collegati alla rete fissa e di reti alternative quali quelle della telefonia mobile che permettano di operare sul *server*/*cloud* senza utilizzare la rete fissa aziendale.

Laddove si proceda con attività di registrazione manuale, l'analisi preventiva dei rischi deve prevedere di presidiare con misure di verifica aggiuntive i passaggi più critici quali sono, ad esempio, le trascrizioni manuali che riguardino la qualifica e la tracciabilità delle unità raccolte. Misure specifiche devono essere predisposte anche per la protezione e gestione dei dati quando siano trascritti su supporti cartacei o conservati su dischi fissi o mobili.

Il materiale presentato in questa sezione è il risultato dell'esperienza maturata da alcuni medici trasfusionisti, in occasione di due attacchi ai sistemi informatici di Aziende Sanitarie italiane avvenuti in maniera indipendente in due diverse realtà, che chiameremo A e B, rispettivamente nel 2021 e 2022. In entrambi i casi si è trattato di attacchi *ransomware* ed hanno coinvolto tutti i computer afferenti alle rispettive reti aziendali. A seguito del primo di questi eventi si è costituito un gruppo di lavoro allo scopo di fare un'analisi retrospettiva dei rischi a cui questi incidenti espongono i ST, valutando la sicurezza ed efficacia delle misure messe in atto così come delle possibili alternative per garantire la continuità delle attività trasfusionali (BC) in caso di interruzione delle reti informatiche e/o di *crash* dei gestionali trasfusionali.

a. Identificazione

In entrambi i casi il *cyber* attacco ha colpito il dominio e la rete di un'Azienda Sanitaria coinvolgendo diversi presidi ospedalieri e tutta la medicina territoriale. Come conseguenza, anche tutte le postazioni informatiche fisse (computer, stampanti) utilizzate dai ST, ubicati nelle Aziende colpite dall'attacco, sono state scollegate dalla rispettiva rete aziendale e quindi rese inutilizzabili per alcune settimane. In questo periodo non è stato possibile utilizzare la rete fissa né per le attività routinarie di raccolta né per la gestione delle richieste trasfusionali. In entrambi i casi il *server* non era residente nella rete aziendale attaccata, questo ha reso possibile sfruttare in parallelo alcune funzionalità by-passando la rete aziendale colpita. In questo senso sono stati inizialmente indentificati quali registrazioni e passaggi di dati potessero essere garantiti usando i terminali ed i canali informatici alternativi sicuri collegati al *server* e quali dovessero

essere invece sostituiti temporaneamente da registrazioni e trascrizioni manuali sugli strumenti o su supporti cartacei.

a. Impatto

Nel caso A, essendoci due Aziende afferenti allo stesso Dipartimento trasfusionale ed essendo il *client-server* dipartimentale localizzato fisicamente nell'Azienda non colpita, è stato possibile continuare ad utilizzare alcune funzioni del sistema informatico trasfusionale dipartimentale mediante la rete della seconda Azienda non coinvolta. Tuttavia la gran parte delle attività di raccolta, lavorazione e qualificazione biologica degli emocomponenti e parte della assegnazione ai reparti era localizzata nell'Azienda interessata dall'attacco e, pertanto, queste attività trasfusionali nelle sedi afferenti sono rimaste prive del supporto informatico diretto, per tutto il tempo in cui i la rete non ha potuto essere riattivata.

Nel caso B, l'attività di lavorazione e qualificazione biologica non sono state coinvolte, perché afferenti ad un'altra rete informatica, così quelle di raccolta mobile ed associativa che utilizzavano per il trasferimento dei dati al server la linea telefonica mobile. Il server in questo caso era localizzato in un *cloud* gestito da un'azienda certificata e qualificata dall'AGID come *cloud service provider*. Ad essere compromesse in questo caso sono state le attività di raccolta e distribuzione di due Ospedali che utilizzavano terminali collegata alla rete colpita dall'attacco.

L'impatto principale in questi due casi ha interessato quindi, *in primis,* il fronte della raccolta e della distribuzione, con la necessità di elaborare modalità alternative per garantire l'identificazione e la tracciabilità delle unità e dei campioni da inviare ai laboratori di qualificazione biologica. In aggiunta, nel caso A, si è posto il problema dell'imputazione sugli strumenti e della trascrizione degli esiti delle indagini di legge per la validazione delle unità.

a. Valutazione

Nell'affrontare questa situazione inattesa il primo problema che si pone è capire l'entità e la gravità del *crash* informatico. A fronte di una situazione non rapidamente ripristinabile, il primo passo è strutturare un percorso decisionale che coinvolga tutti i centri direttamente o indirettamente colpiti dal blocco e la Struttura Regionale di Coordinamento per le attività trasfusionali (SRC) con funzioni di coordinamento, per l'organizzazione di un iniziale supporto, se necessario, alle Aziende colpite, attraverso l'invio di unità di emocomponenti raccolte e validate da altri ST regionali ma anche per la gestione dei rapporti con le SRC di altre Regioni, al fine di garantire le attività ospedaliere essenziali. Il percorso logico è sintetizzato nella Figura 3 e prevede una iniziale sospensione di tutte le attività della filiera trasfusionale coinvolte dal blocco dei sistemi informatici, ad eccezione dell'assegnazione degli emocomponenti che, come già accennato, mantiene l'operatività grazie all'attivazione del protocollo locale di distribuzione senza supporto informatico, come previsto dal DM 2 novembre 2015. Sono stati necessari alcuni giorni per prendere atto dell'entità del problema e soprattutto del livello di incertezza sui tempi di riattivazione dei collegamenti informatici.

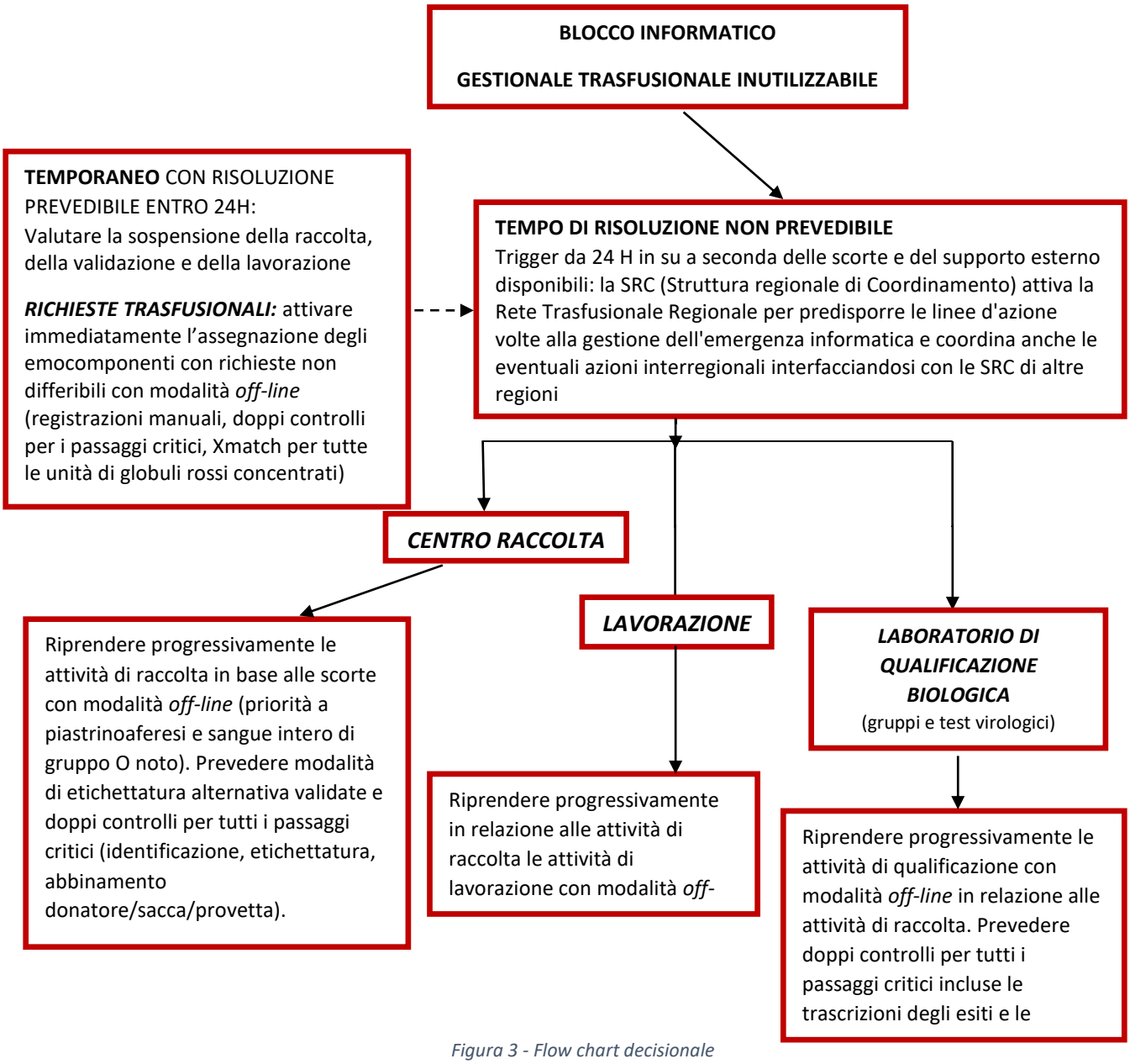

Figura 3 - Flow chart decisionale

b. Trattamento Immediato

Per garantire nel breve periodo le attività essenziali della filiera trasfusionale, date le differenze di contesto e di risorse tecnologiche, le strategie utilizzate nei due casi sono state diverse.

Caso A

Non avendo altre opzioni, dopo le prime 24 ore, è stato elaborato un primo protocollo di raccolta che prevedeva una modalità di etichettatura temporanea in manuale, con un doppio controllo da parte degli operatori, mentre l'accettazione informatica avveniva successivamente, trasportando celermente le unità e le provette presso la sede non dipendente dalla rete aziendale colpita, dove venivano generate le etichette per sacche e provette e si provvedeva quindi alla loro rietichettatura. Questi due delicati passaggi, accettazione e rietichettatura, erano presidiati con due operatori. Inizialmente ci si è concentrati sulla raccolta delle piastrine da aferesi e, progressivamente, sulla base delle scorte monitorate manualmente quotidianamente, si è provveduto a riprendere anche la raccolta di sangue intero, cominciando dai donatori di gruppo 0 noto. Le indagini per la qualificazione biologica sono state eseguite sugli strumenti con

modalità *offline*, caricando i campioni tramite il codice numerico unico delle etichette generate nella seconda accettazione e inserendo gli esami manualmente. I risultati dello strumento venivano poi trasferiti su supporti mobili e stampati utilizzando stampanti non collegate alla rete. La trascrizione degli esiti delle indagini di qualificazione biologica veniva eseguita, come per l'accettazione, inserendo manualmente gli esiti nel gestionale dipartimentale dell'Azienda non colpita ed anche questo passaggio è stata presidiato con doppio controllo indipendente da parte di due operatori. Le procedure di distribuzione e di assegnazione non si sono mai interrotte ed è stato applicato sin da subito il protocollo previsto in questi casi dalla norma, producendo tutta la documentazione cartacea per garantire tracciabilità, sicurezza e ricostruibilità del percorso informatizzato una volta ripristinato il sistema.

Caso B

In questo caso tutte le attività di raccolta ed assegnazione sono state rapidamente riallineate utilizzando come terminali i computer portatili, già in uso per le unità di raccolta mobili e per la telemedicina, adeguatamente configurati direttamente alle stampanti di etichette per sacche e provette. Il collegamento al server, come avveniva già per le raccolte mobili, è stato garantito tramite router 4G collegato alla rete telefonica mobile. Anche per quanto riguarda la distribuzione si è proceduto in maniera analoga, usando computer portatili collegati via etere alla telefonia mobile. Come accennato, la presenza di un *server* in *cloud*, gestito da ente terzo certificato, ha garantito la piena funzionalità di raccolta e lo avrebbe fatto anche in caso di *crash* di tutte le reti fisse aziendali.

c. Misure preventive e "Disaster Plan"

Come accennato, dopo il primo incidente è stato formato un gruppo di lavoro con il fine di fare una revisione sistematica di quanto fatto e più in generale con l'obiettivo di elaborare ulteriori misure preventive da utilizzare nel caso di situazioni analoghe che colpissero i sistemi gestionali trasfusionali.
Le proposte emerse sono state sintetizzate nella Tabella 1, che è strutturata come una lista di verifica – *checklist* di requisiti da soddisfare – accompagnata da una valutazione semplificata dei diversi livelli di rischio (alto o moderato) a cui può esporre l'impiego di procedure alternative manuali e/o offline, ovvero utilizzando computer non collegati alla rete e quindi al *server*.

Sono state definite ad alto rischio tutte quelle fasi e quei passaggi che, in caso di errore nell'esecuzione o trascrizione in modalità manuale/*offline*, potessero portare a:

- un'errata attribuzione dello stato di qualificazione degli emocomponenti prodotti (qualifica del donatore, indagini "di legge" di qualificazione biologica);
- la perdita della corretta tracciabilità donatore - paziente.

Per i passaggi valutati ad "alto rischio" le procedure specifiche devono prevedere come minimo un doppio controllo, indipendente e documentato, da parte di due operatori qualificati.
Nella terza colonna della Tabella 1 sono riportate una serie di possibili soluzioni operative, alcune delle quali utilizzate sul campo, dalle due Aziende Sanitarie, nei casi degli incidenti descritti, altre possibili soluzioni sono state elaborate successivamente. Queste soluzioni operative sono state pensate per ridurre i rischi legati alla operatività in modalità manuale/*offline* durante i vari passaggi del percorso da vena a vena.
I contenuti della tabella, in particolare l'analisi dei rischi e delle misure e soluzioni previste, non pretendono di essere esaustivi ed appropriati in tutti i contesti, ma hanno l'obiettivo di stimolare la riflessione e la ricerca di soluzioni più efficaci possibili che devono essere disegnate sulla base dell'analisi dei rischi calata nello specifico contesto organizzativo in cui ciascun gruppo di lavoro opera.

Come riflessione finale, anche sulla base di quanto emerso nel secondo incidente, durante il quale la funzionalità del sistema informatico è stata rapidamente ripristinata nonostante il persistere della interruzione dei flussi informatici aziendali, è importante sottolineare come, a livello strutturale, i ST dovrebbero avere in dotazione sistemi alternativi (*hardware*, rete, *server*) convalidati, conservati *offline*, se

necessario periodicamente aggiornati, che possano essere messi in uso ed allineati in tempi rapidi con il *sever* e gli strumenti. Nel caso B infatti, la disponibilità di computer portatili e stampanti collegati al server tramite rete mobile, abbinata alla presenza di un *server* in *cloud*, certificato e gestito da terzi, ha permesso di garantire la BC delle attività di raccolta e distribuzione in piena sicurezza con il supporto del sistema informatico.

In dettaglio, la dotazione di *backup* di sistema alternativo dovrebbe prevedere:

- computer portatili per utilizzare i gestionali trasfusionali che sono mantenuti scollegati dalla rete e pre-configurati per collegarsi direttamente alle stampanti ed agli strumenti/*middleware* senza utilizzare la rete fissa;
- stampanti di etichette collegate direttamente ai computer portatili;
- connessioni di rete collegate a router 4G/5G della rete di telefonia mobile che possano mettere in comunicazione i terminali con il server;
- server in *cloud* (fuori dalla rete locale) con solidi sistemi di *backup* a *server mirroring*.

Tabella 1 Requisiti, rischi e strumenti/soluzioni

Requisiti	**Livello Rischio**	**Possibili Strumenti/Soluzioni**
1. CENTRO RACCOLTA	*Predisposizione e convalida di una procedura per garantire le attività di raccolta in caso di blocco informatico prolungato. La procedura dovrebbe prevedere le modalità di etichettatura che permettano la lettura strumentale delle unità e delle provette e garantire la piena tracciabilità da donatore a ricevente delle attività di convalida e di assegnazione*	
1.1 É disponibile una modalità *offline* per identificare il donatore ed abbinare in maniera univoca l'unità donata ed i relativi campioni biologici	**RISCHIO ALTO**	• Messa in utilizzo di computer portatili con relative stampanti e lettori ottici non collegati alla rete che possano collegarsi al *server* utilizzando la rete di telefonia mobile (router 4/5G) **Se ciò non è possibile prevedere alcuni dei seguenti strumenti:** • Registro cartaceo/elettronico *offline* di donazione con dati identificativi paziente e CDM • Sistema di identificazione del paziente presidiata in tutte le fasi della donazione • Sistema *offline* con stampa di barcode con CF/CDM gestibili dagli strumenti • Etichette con CDM/identificativo univoco prestampate dotate di codice a barre per unità e provette • Etichette con CF/dati in chiaro generato da sistema *offline* per etichettatura provvisoria delle unità ai fini della identificazione del donatore • Attribuzione di codifica autoportante tramite PC portatile *offline* con link tra codice fiscale e codice donazione temporanea da riportare anche su tutte le provette (link uno a uno)
1.2 Le etichette sono correttamente applicate e contengono tutte le informazioni richieste (centro raccolta, data di raccolta, data di scadenza)	**RISCHIO ALTO**	Solida procedura di predisposizione delle etichette e successiva etichettatura con sistemi offline che preveda la presenza del doppio controllo di tutti gli elementi identificativi critici.

1.4 Sono previsti sistemi per registrare l'invio delle unità al centro di lavorazione e dei campioni al centro di qualificazione biologica	**RISCHIO MODERATO**	• Registro di scarico/carico manuale o con lettura barcode *offline*. • Predisposizione di file semplici con codice donazione ed esami standard di qualificazione
1.5 Le informazioni per il rilascio delle unità riguardanti l'idoneità del donatore alla donazione e le condizioni di conformità della raccolta vengono registrate.	**RISCHIO ALTO**	• Registro di *release* delle unità dopo verifica documentata e tracciata del questionario anamnestico e della procedura di raccolta da parte del responsabile della raccolta • Registro che contiene la lista delle unità raccolte ma non idonee e le evidenze della loro eliminazione • Registro di scarico manuale/elettronico con sistema *offline*
2. CENTRO LAVORAZIONE	*Predisposizione e convalida di una procedura che garantisca le attività di lavorazione di in caso blocco informatico prolungato che permetta la tracciabilità e registrazione di tutte le fasi critiche*	
2.1 Sono garantite le registrazioni necessarie a documentare il corretto trasporto delle unità da/al centro di Lavorazione	**RISCHIO MODERATO**	• Registro di trasporto compilato a mano • Modalità di registrazione delle temperature gestibile offline
2.2 La tracciabilità delle unità durante la lavorazione viene garantita	**RISCHIO MODERATO**	• Registro di lavorazione in manuale • Acquisizione di elenchi file semplici generati offline
2.3 I dati di scomposizione vengono registrate	**RISCHIO MODERATO**	• File prodotti dagli scompositori temporaneamente collegati a PC portatili con *software* locale • Registri Manuali
2.4 I dati di congelamento vengono registrati	**RISCHIO MODERATO**	• Monitoraggio con registrazione manuale delle temperature e tempi di congelamento • Modulo di registrazione processo di congelamento per batch • Registrazione autonoma degli abbattitori senza trasferimento a gestionale

2.5 Le unità valide sono identificate e rilasciate correttamente.	**RISCHIO ALTO**	Registro *di release* delle unità dopo verifica documentata e tracciata del percorso di lavorazione, della ammissibilità anamestica del donatore, dell'esito degli esami di qualificazione biologica e dell'emocromo da parte del personale responsabile del rilascio. • Etichette di validazione sacche generate offline / prestampate • Utilizzo di etichette di gruppo AB0 Rh prestampate. • Doppia verifica di etichettatura di gruppo • Robusta procedura di etichettatura e verifica delle unità valide con doppio controllo
3. CENTRO DI VALIDAZIONE BIOLOGICA	*Predisposizione e convalida di una procedura che garantisca la sicurezza delle attività di qualificazione biologica (gruppaggio, virologia e NAT) in caso blocco informatico prolungato. La procedura dovrebbe prevedere la tracciabilità, la documentazione della corretta esecuzione delle indagini, della corretta trascrizione e registrazione degli esiti delle indagini di qualificazione ai fini del rilascio finale delle unità (rif. 2.5)*	
3.1 È garantita la corretta attribuzione delle provette al donatore, alla donazione e la corretta richiesta delle indagini di qualificazione (gruppo e virologia, NAT) .	**RISCHIO ALTO**	• Messa in utilizzo di computer portatili con relative stampanti e lettori ottici non collegati alla rete che possano collegarsi al server utilizzando la rete di telefonia mobile (router 4/5G) e predisposti a trasferire dati per e da gli strumenti analitici/middleware senza utilizzare la rete fissa. **Se ciò non è possibile prevedere alcuni dei seguenti strumenti:** • Utilizzo di Etichette con codice a barre linkate in maniera univoca alle unità raccolte ed al donatore (vedi 1.1) • Presenza di file cartaceo/informatico (generato offline) di accompagnamento in cui sia presente l'abbinamento delle provette alla donazione ed alle le indagini richieste (vedi 1.1) • Inserimento manuale sullo strumento utilizzando gli identificativi, se possibile con utilizzo di codice a barre, attribuiti in sede di donazione, e l'esame richiesto.

3.2 Gli esiti degli esami di qualificazione biologica vengono correttamente registrati ed attribuiti agli emocomponenti prodotti.	**RISCHIO ALTO**	• Produzione di un report riassuntivo di seduta analitica che contenga:
		  • gli esiti delle indagini generate dagli strumenti;
		  • la corretta attribuzione alle corrispondenti unità.
		• Per ogni trascrizione deve essere prevista una doppia verifica indipendente da parte di due operatori
		• Valutare la possibile stampa dei risultati direttamente dallo strumento su stampante offline, salvataggio file su chiavetta USB (prevedere gestione protetta dei dati)
		• Valutare il possibile utilizzo di funzioni *middleware* non collegate a gestionale e su *server* indipendenti che permettano di produrre un registro di qualificazione biologica
		• Preliminare *check* in doppio sugli esiti virologici reattivi, attivazione di sistema rapido di registrazione, identificazione e notifica al centro di lavorazione per l'eliminazione delle unità coinvolte.

4. ASSEGNAZIONE DEGLI EMOCOMPONENTI	*Predisposizione e convalida di una procedura che garantisce le attività di assegnazione degli emocomponenti ai pazienti di in caso blocco informatico prolungato e la corretta conservazione degli stessi (registrazione temperatura e gestione allarmi remotizzati). La procedura deve prevedere modalità controllate e sicure per la assegnazione corretta di unità compatibili e le relative registrazioni al fine di garantire la piena tracciabilità*	
4.1 La presa in carico degli emocomponenti è registrata e vi è un sistema di gestione controllata delle scorte.	**RISCHIO MODERATO**	• Messa in utilizzo di computer portatili con relative stampanti e lettori ottici non collegati alla rete che possano collegarsi al server utilizzando la rete di telefonia mobile (router 4/5G) **Se ciò non è possibile prevedere alcuni dei seguenti strumenti:** • Registro di carico emocomponenti manuale o elettronico con lettore di barcode • Conferma di validità su registro di carico a seguito di verifica crociata su copia registro di validazione • Modalità di back-up dei sistemi di controllo della temperatura e relativi allarmi

4.2 Le richieste trasfusionali sono gestite in modalità offline garantendo le registrazioni e la documentazione necessaria	**RISCHIO ALTO**	• Richiesta trasfusionale cartacea accompagnata da copia CF paziente (se disponibile) • Solida procedura di etichettatura da parte dei reparti richiedenti ed eventuale rietichettatura con sistemi *offline* con utilizzo di codici a barre per lettura strumentale • Considerare la predisposizione di un file salvato ogni giorno su memoria esterna fissa (valutare problematiche di privacy) con archivio anagrafiche gruppi e TCI pazienti degli ultimi mesi/anni. • Considerare tutti i pazienti come nuovi, doppia provetta per tutti, Gestione in manuale utilizzando la richiesta come documento dove registrare l'esito degli esami e le unità assegnate. • Valutare opportunità di passare in modalità crociata per tutte le richieste
4.3 Le indagini pretrasfusionali vengono registrate in maniera corretta.	**RISCHIO MODERATO**	• Foglio di lavoro stampato dallo strumento con modalità *offline* • Copia delle richieste trasfusionali con trascrizione degli esiti indagini delle indagini di compatibilità archiviate in maniera ordinata e tale da poter essere facilmente rintracciate • Sistema informatico offline con archivio anagrafiche gruppi e TCI pazienti registrate in un intervallo di tempo definito
4.4 Le unità di emocomponenti vengono correttamente assegnate sulla base delle prove pretrasfusionali.	**RISCHIO ALTO**	• Etichette adesive da compilare a mano con abbinamento al paziente, con data, ora e identificativo dell'operatore • Sistema informatico offline che stampa abbinamento • Utilizzo *middleware* strumentale degli strumenti di immunoematologia
4.5 L'avvenuto scarico ai reparti e la successiva avvenuta trasfusione vengono registrati.	**RISCHIO MODERATO**	• Registro cartaceo di scarico, con attribuzione dell'unità a paziente, reparto • Registro elettronico offline di scarico

4. Misure di protezione dei dati informatici

Quali sono le modalità di accesso ed i comportamenti corretti nell'utilizzo dei sistemi informatici da parte degli operatori?

Per la sicurezza dei sistemi e la protezione dei dati, l'accesso a tali sistemi informativi sanitari deve avvenire solo da parte di utenti autorizzati attraverso modalità di identificazione sicura, secondo i livelli di sicurezza previsti dalle normative, quali *login* e *password* con precise specifiche (OTP, SPID, ecc.). Risulta inoltre fondamentale che gli operatori che accedono ai sistemi ed alle reti informatiche dei servizi sanitari non espongano, con utilizzi inappropriati e non sicuri, i sistemi informatici ed i dati ivi contenuti a minacce esterne. In questo senso è disponibile ed accessibile online una dettagliata linea guida emanata dall'Istituto Superiore di Sanità "Buone pratiche per la sicurezza informatica nei servizi sanitari".

Di seguito si illustrano le attività afferenti alla protezione dei dati personali a cui è necessario adempiere nel caso di raccolta, lavorazione, qualificazione biologica e gestione delle richieste trasfusionali, per evitare che in caso di *cyber attack* il sistema informatico venga reso di fatto inutilizzabile in un'Azienda sanitaria colpita da un attacco *hacker*, che ha reso inutilizzabile la rete dei sistemi informatici utilizzati allo scopo. Ciò a maggior ragione considerato che la riorganizzazione delle attività produttive determina la riduzione in pochi punti strategici di tutta l'attività di qualificazione biologica e di lavorazione degli emocomponenti per intere regioni. Un blocco operativo potrebbe essere gravissimo in termini di interruzione dei livelli essenziali di assistenza trasfusionali e, più in generale, della capacità di assistenza sanitaria ai cittadini. Il capitolo si compone di due parti, i cui contenuti afferiscono sia agli aspetti propriamente informatici sia a quelli dedicati alla protezione dei dati.

a. Architettura tecnologica finalizzata ad assicurare continuità e sicurezza dei dati trattati dalle Strutture Trasfusionali Italiane.

Al fine di garantire il massimo grado di sicurezza per i dati trattati e la indispensabile continuità operativa dei ST, che garantiscono l'approvvigionamento di emocomponenti labili ed emoderivati, l'infrastruttura tecnologica che ospita il Sistema gestionale informatizzato (SGI) del ST dovrebbe essere basata su una architettura *web-based n-tier*, con adozione di stili architetturali che prevedano la possibilità di gestire in modo flessibile processi, ruoli e regole di *business* attraverso configurazioni di moduli o *system software* dedicati, senza necessariamente intervenire sul codice sorgente.

La soluzione non dovrebbe prevede l'utilizzo di *application broker* per la fruizione tramite *web browser* della componente *client* di una architettura applicativa *software client/server*. Dovrebbe prevedere la possibilità di configurare il sistema per garantire la scalabilità, ovvero la proprietà di un sistema di crescere o decrescere in base alle esigenze e alle necessità, sia verticalmente, intervenendo su di un singolo server incrementando o riducendo le risorse computazionali (vCPU, RAM, HD, ...), sia orizzontalmente, intervenendo sulla struttura del sistema aggiungendo o eliminando *server*.

La soluzione deve fare riferimento alle linee guida dell'AGID circa le "Misure minime di sicurezza ICT per le pubbliche amministrazioni"[3] e le "Linee guida AGID per lo sviluppo del software sicuro"[4]. L'installazione del SGI dovrebbe essere prevista in *cloud* (IaaS) su soluzioni di *Web Farm* con certificazioni quali ISO 27001:2013 e conformi ai controlli previsti dalle norme ISO 27017:2015 e ISO 27018:2014, ISO 20000-1 e ISO 22301. Per la soluzione infrastrutturale sono auspicabili qualificazioni come CSP (*Cloud Service Provider*), accreditamento AGID con infrastrutture riconosciute da AGID come candidabili ad essere utilizzate dal Polo Strategico Nazionale, se disponibile certificazione Tier III secondo lo standard ANSI TIA 942. La soluzione deve garantire elasticità e continua disponibilità delle risorse, anche distribuite geograficamente, senza alcuna ripercussione sugli utenti del sistema. La soluzione dovrà essere implementata per garantire una distribuzione geografica delle componenti applicative e una replica asincrona della componente di DBMS (*Database Management System*) in modo da rendere disponibile il servizio agli utenti anche nel caso di indisponibilità di una intera *Availability Zone*. La soluzione dovrà pertanto garantire l'installabilità su almeno due *Availability Zone* e il completo allineamento sia *software* che infrastrutturale fra le due *Availability Zone* (schema *active-passive*).

- **Per garantire la sicurezza di accesso degli operatori**, la soluzione dovrebbe disporre di un sistema di autenticazione e autorizzazione modulare compatibile con sistemi di autenticazione federata basata sul protocollo SAML2 per gli accessi via web. La soluzione proposta deve essere integrabile con un *Identity Provider* esterno. Tale soluzione, basata sulla modalità MFA, deve consentire la gestione dei profili degli utenti con accesso multiutente, con profilazioni differenziate, e la gestione di un'anagrafica degli utenti.
- **Per garantire il controllo sulla sicurezza ed integrità dei dati**, devono essere disponibili i risultati dei test di vulnerabilità della soluzione, effettuati periodicamente, per le istanze già installate.

Il Fornitore dovrà porre in essere:

- un *vulnerability assessment* sia di tipo infrastrutturale sia applicativo, periodico ad intervalli minimi di sei mesi, che includa il *Penetration test*;
- la tempestiva applicazione di *patch* di sicurezza sia nel *software* applicativo sia nei *middleware* utilizzati, pubblicate periodicamente dalle case madri dei prodotti utilizzati (compresi i *firmware*) nel rispetto dei comunicati effettuati dagli organismi internazionali di sicurezza (principalmente i CERT - *Computer Emergency Response Team*), relativi alle nuove vulnerabilità.

Il Fornitore garantisce il rispetto della normativa internazionale in materia di sicurezza ICT. Sono prontamente evidenziate e comunicate le situazioni legate a tentativi di violazione della sicurezza (accessi anomali, brute force attack, ecc.) ed eventuali *data breach*, nella forma e secondo le modalità previste dal Regolamento UE 2016/79 GDPR, avendone regolamentato i processi e avendo individuato i propri riferimenti, che possano riferire all'ente appaltatore in caso di violazioni/attacchi e garantire il corretto supporto e comunicazione.

Dovranno essere previsiti e disponibili i risultati dei test di carico (Stress Test) della soluzione.

A tal fine, i server virtuali sono in esecuzione sia su piattaforma *OpenStack* che su piattaforma vSphere (o soluzioni equivalenti) in funzione dei template prescelti. Tutti i dischi/file system dei server virtuali devono

[3] Circolare 18 aprile 2017, n. 2/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». GU – Serie generale n. 103 del 5/5/2017.

[4] "Linee guida di sicurezza nello sviluppo delle applicazioni", disponibili all'indirizzo URL: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lineeguidasicurezza-introduzione.pdf

essere salvati su *datastore* messi a disposizione dalla *Storage Area Network*. Nel dettaglio si tratta di un'area composta da più *server Storage* centrali collegate alle differenti infrastrutture virtuali tramite fibra ottica. Ogni *datastore*, definito su infrastruttura virtuale, ha più *path*, in modo da evitare *single point of failure* in caso di guasto di una fibra ottica, porta *switch* o porta *server* fisico. I dischi su *storage* sono configurati in RAID con *hot spare* in modo che, in caso di guasto di un disco, questo passi automaticamente in stato di *fault* e sia sostituito da altro disco senza alcun disservizio o perdita di dati.

- **Backup:** in questo tipo di soluzione, tutti gli strumenti di *backup* vengono messi a disposizione dall'infrastruttura stessa senza intervento del fornitore del *software* o dei sistemisti delle Aziende o dei ST. Soluzioni di questo tipo consentono tempi di RTO di gran lunga inferiori alle 24 ore garantendo di fatto una BC quasi assoluta (vedi Cap. 2 per i dettagli già descritti)
    - **Garanzia di continuità operativa del collegamento di rete**: alla luce dei recenti attacchi che hanno spesso compromesso le reti aziendali, rendendole di fatto non utilizzabili, deve essere prevista, per i ST, la realizzazione e messa a disposizione di una rete di *backup*, sia *wired* sia *wireless,* che consenta di raggiungere in ogni condizione i server collocati in *cloud*. La rete dovrebbe avere caratteristiche tali da poter garantire la funzionalità prevista in ogni condizione, pertanto si ritiene preferibile una rete basata su tecnologia 4 o 5G. Deve essere prevista un'adeguata dotazione *hardware* costituita da Router 4 o 5 G, PC dotati di relativa connettività e stampanti sia per modulistica che per etichette, tali da garantire, in termini numerici, le principali attività di una struttura trasfusionale, così come definite nei requisiti di accreditamento istituzionale: a titolo esplicativo non esaustivo, raccolta, qualificazione biologica, produzione emocomponenti, assegnazione e consegna emocomponenti, distribuzione ad altri ST collegati, funzioni centralizzate di secondo livello. Sia i computer che i relativi apparati di rete necessari per il collegamento 4 o 5G (router, *firewall*, ecc..) devono essere mantenuti totalmente scollegati dalla rete aziendale al fine di evitare qualunque possibile attacco informatico. Inoltre devono essere periodicamente aggiornati sia per quanto riguarda il sistema operativo sia per i sistemi di rilevamento antivirus e simili. La periodicità deve essere tale da garantire sempre il perfetto funzionamento (indicativamente almeno settimanale) e deve essere gestita evitando comunque l'utilizzo della rete aziendale. I computer di riserva devono naturalmente essere in grado di accedere a tutte le funzioni del gestionale trasfusionale, garantendo anche la relativa stampa di report, etichette e registri, ove richiesti. Al fine di garantire tutta la filiera "da vena a vena", le strutture che gestiscono gli esami di qualificazione biologica e la produzione, devono essere in grado di operare con i sopradescritti sistemi tramite 4 o 5G anche per quanto riguarda il collegamento delle singole strumentazioni ai server che ospitano i *middleware* per i quali deve essere prevista l'installazione in *cloud*. Tutta l'infrastruttura di riserva deve poter essere mantenuta in *stand by* ed attivata solo dopo un eventuale attacco alla rete aziendale. Risulta pertanto necessaria la verifica preventiva che le strumentazioni utilizzate, ove collegate al sistema informatico possano essere gestite da una doppia linea di computer alternativi tra loro. Quelli tenuti in *stand by* devono poter essere attivati, collegati a tutta la strumentazione, pre-configurati per il collegamento al router 4 o 5G ed essere in grado di raggiungere, tramite tale collegamento di riserva, il *cloud* ove risiede di norma il *middleware* strumentale o, in caso di non utilizzo di *middleware*, possano raggiungere direttamente il server ove risiede il SGI. I *middleware* strumentali, avuta presente l'architettura prevista per la gestione dei server del SGI trasfusionale, dovrebbero essere ospitati in cloud eventualmente nella stessa *web farm* certificata che ospita il SGI trasfusionale, per offrire la

massima garanzia di interoperabilità e BC dell'interfaccia strumentale stessa al gestionale. La logica di configurazione ed il dimensionamento dei server da dedicare complessivamente al sistema sopra descritto deve essere oggetto di un adeguato e documentato *risk assesment* predisposto dalla ditta che fornisce il servizio *cloud* in accordo con i requisiti predefiniti (*user requirements*) dal fornitore del gestionale trasfusionale e dal fornitore dei sistemi strumentali utilizzati per la qualificazione biologica, per la produzione e assegnazione degli emocomponenti.

I requisiti a garanzia della BC descritti nel presente documento devono essere previsti nelle gare per la fornitura delle strumentazioni a supporto dei processi trasfusionali e devono essere oggetto di specifica verifica prima di rendere effettiva la fornitura stessa. Inoltre devono essere oggetto di convalida.

b. *Procedura finalizzata ad assicurare la corretta gestione dei dati personali in aderenza alla normativa europea e nazionale (Regolamento EU 679/2016 e d.lgs. 101/2018)*

Riportare sul registro dei trattamenti di competenza le attività di raccolta e di gestione dei dati personali operate manualmente. Nel contesto del documento si indicherà anche il livello di rischio afferente alla procedura di trattamento manuale prescelta.

Elaborare una policy esplicativa dei comportamenti da adottare sotto il profilo afferente la tutela della privacy, nell'ambito dei trattamenti dei dati personali gestititi al di fuori del gestionale trasfusionale, che fornirà agli operatori le opportune indicazioni in ordine:

I. alla corretta conservazione dei registri utilizzati per la raccolta dei dati personali del paziente. Particolare cura verrà riposta nell'indicazione delle procedure di conservazione del registro al termine delle attività operative e alle misure adottate per la assicurare la custodia dello stesso in ambiente sicuro (armadi con chiusura a chiave, in stanze con accessi limitati e controllati, etc.).
II. Alla corretta conservazione del registro afferente la raccolta, la lavorazione e la qualificazione biologica. Anche in tale contesto verrà data particolare attenzione nell'indicare le misure di sicurezza adottate per la custodia dello stesso.
III. Alla corretta produzione e conservazione dei *barcode* generati *off-line* con stampanti non collegate alla rete. I dati eventualmente conservati nella memoria della stampante saranno distrutti non appena le emergenze verranno risolte. In tale contesto dovrà risultare per iscritto l'avvenuta distruzione.
IV. All'adozione di una politica *"green desk"* che richiami costantemente gli operatori sulla necessità di liberare le scrivanie e i supporti presenti nei luoghi di lavoro da tutta la documentazione contenente dati personali al termine delle operazioni giornaliere. In tale ambito sarà utile richiamare la sensibilità del Responsabile del ST.
V. Ad assicurare la conservazione dei dati personali su supporto cartaceo generato manualmente o con *device* non collegato alla rete, in armadi o cassetti chiusi a chiave ed accessibili solo da personale autorizzato. La *policy* che verrà redatta in proposito indicherà i nominativi e le funzioni del personale dedicato alla specifica attività.
VI. Ad indicare nominalmente nell'ambito della *policy*, le persone responsabili della custodia delle chiavi idonee all'accesso nei luoghi di lavoro.

VII. Al ripristino dell'operatività della rete, i dati personali raccolti manualmente dovranno essere digitalizzati e riportati sul gestionale trasfusionale. Al termine della suddetta operazione gli stessi verranno distrutti o anonimizzati.

Allegato 1 – Riferimenti normativi

1. *Le norme europee in materia di cybersecurity*

- ***2013*** – Istituzionalizzazione Agenzia dell'Unione europea per la cibersicurezza (ENISA)[5] – ridefinisce ed accresce l'importanza dell'agenzia europea per la sicurezza delle reti e dell'informazione.
- ***2014*** – Regolamento eIDAS[6] (*electronicIDentificationAuthentication and Signature*) - definisce in modo univoco l'identità nel settore digitale e il valore probatorio delle comunicazioni e dei documenti informatici.
- ***2016*** – Direttiva NIS[7] - definisce le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Viene imposta, a tutti gli Stati che fanno parte dell'Unione, l'adozione di misure comuni e strategiche per la sicurezza delle reti e dei sistemi informatici.
- ***2019*** – *CybersecurityAct*[8] - Centralizza in ambito *cyber* il ruolo di ENISA nella definizione dei parametri chiave della sicurezza, del coordinamento dell'operato dei vari stati membri e dei processi di certificazione.

2. *Le norme nazionali in materia di cybersecurity*

Gli interventi sopra citati hanno costituito la cornice per definire il quadro normativo nazionale che si può sintetizzare come segue:

- ***Decreto legislativo (D.lgs.) 26 agosto 2016 n. 179***[9] – contiene modifiche ed integrazioni al Codice dell'Amministrazione Digitale in materia di riorganizzazione delle amministrazioni pubbliche.
- ***D. lgs. 18 maggio 2018***, n. 65[10] (anche detto "decreto legislativo NIS"), in vigore dal 24 giugno 2018 – attua la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
- ***DPCM dell'8 agosto 2019***[11] – Disciplina l'organizzazione ed il funzionamento del CSIRT che ha cominciato ad operare il 6 maggio 2020 in sostituzione del CERT Nazionale e del CERT-PA.
- ***Decreto-legge 21 settembre 2019***, n. 105 convertito in L. 18 novembre 2019, n. 133[12] – contiene disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.
  In attuazione del citato Decreto si segnalano i seguenti:

[5] *Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004*
[6] Regolamento UE n° 910/2014 sull'identità digitale - base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.
[7] DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
[8] REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)
[9] Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2016/09/13/16G00192/sg
[10] Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg
[11] Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg
[12] Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg

- Decreto del Presidente del Consiglio dei Ministri (DPCM) n. 131 del 30 luglio 2020[13] – individua i parametri con cui sono individuati i soggetti che svolgono funzioni essenziali per lo Stato.
- DPCM n. 14 aprile 2021, n. 81[14] – individua le categorie gli incidenti aventi impatto sui beni ICT.
- DPCM del 15 giugno 2021[15] – individua le categorie di beni ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica.

- ***Decreto-legge 14 giugno 2021***, n. 82[16] – contiene disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

3. Il contesto normativo italiano in ambito cybersecurity

Nel 2013, con il cd. "Decreto Monti", l'Italia ha delineato per la prima volta la sua "postura" di sicurezza cibernetica, provvedendo a sistematizzare, sia pure con la legislazione vigente, le molteplici competenze di settore distribuite tra diversi attori istituzionali.[17] Ciò ha consentito l'avvio dell'accrescimento delle capacità *cyber* nazionali attraverso gli atti di indirizzo strategico e operativo.

Successivamente, la sopra citata Direttiva NIS ha imposto la verifica sia dell'efficacia dell'architettura nazionale, a fronte della crescente sofisticazione della minaccia e della rilevanza strategica dei target cui la stessa si rivolge sia degli impegni assunti dall'Italia in ambito internazionale. Gli esiti di tale verifica sono stati sintetizzati nel cosiddetto "DPCM Gentiloni" che, ad invarianza del quadro normativo primario vigente, è intervenuto razionalizzando ulteriormente l'architettura delineata nel precedente decreto sopracitato. Tale provvedimento ha ridefinito le attribuzioni del Presidente del Consiglio dei Ministri e del CISR nel campo della sicurezza cibernetica, in linea con le funzioni di deliberazione, consulenza e proposta, a supporto del Presidente del Consiglio attribuite al CISR dall'articolo 7bis del decreto-legge n. 174/2015 in caso di crisi, assegnando al Direttore Generale del Dipartimento delle informazioni per la sicurezza (DIS) un ruolo attivo e centrale nella gestione ordinaria e straordinaria della *cybersecurity* in Italia. Questi, infatti, è chiamato a definire le linee di azione di interesse generale, al fine di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti nazionali e ad individuare le più avanzate soluzioni tecnologiche a sostegno delle attività di prevenzione, contrasto e risposta agli incidenti che interessino amministrazioni, enti pubblici e operatori privati.[18]

Negli ultimi anni è seguito un riassetto a livello nazionale che ha consentito di sviluppare proficuamente le iniziative comunitarie, in linea con quanto fatto da altri Paesi tecnologicamente avanzati, attraverso un nuovo soggetto istituzionale in grado di fungere da stimolatore, collettore e incubatore. Alla nuova Agenzia nazionale per la sicurezza cibernetica è stato pertanto affidato il compito di dare vita ad un'effettiva alleanza tra istituzioni, aziende e mondo accademico, così da favorire lo sviluppo di linee di ricerca mirate nell'ottica di delineare appropriate architetture digitali nazionali intorno al concetto di sicurezza, in grado di rispondere, in un contesto di profonda trasformazione digitale, alla complessità delle minacce presenti e future, e assicurare una "continuità di servizio", che possa abilitare un organico sviluppo economico e sociale del Paese.

[13]Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg
[14]Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg
[15]Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg
[16]Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg
[17]Disponibile all'URL: https://www.gazzettaufficiale.it/eli/id/2012/03/24/12A03524/sg
[18]Cfr. DIS all'URL: http://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html

a. Il recepimento della Direttiva NIS in Italia

L'Italia ha dato attuazione alla Direttiva NIS (UE) 2016/1148, recependola nell'ordinamento nazionale, con D. lgs. 18 maggio 2018, n.65.

In ambito nazionale, al fine di agevolare le Autorità competenti NIS nell'adempimento dei compiti loro affidati, è stato istituito, attraverso un apposito DPCM, un Comitato tecnico di raccordo. Il Comitato opera presso la Presidenza del Consiglio dei ministri, riunendo i delegati dei Ministeri-Autorità competenti NIS e i rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. A seguito del recepimento della Direttiva NIS, è stata formulata la *Strategia nazionale di sicurezza cibernetica*[19], adottata dal Presidente del Consiglio dei ministri, sentito il CISR.

b. Obblighi in materia di sicurezza

Il decreto attuativo ripropone gli obblighi generali di sicurezza previsti dalla Direttiva NIS all'articolo 14. In sostanza, gli OSE sono tenuti ad adottare misure tecnico-organizzative adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici. Il decreto specifica che nell'adottare tali misure gli operatori sono tenuti a tenere in debita considerazione le linee guida predisposte dal Gruppo di Cooperazione nonché le linee guida predisposte dalle autorità competenti NIS. Tali linee guida acquisiscono quindi un'importanza fondamentale ai fini di dimostrare l'adeguatezza delle misure adottate.

Analoghi obblighi in materia di sicurezza sono previsti a carico dei fornitori di servizi digitali, specificati nel Regolamento di esecuzione (UE) 2018/151 della Commissione del 30 gennaio 2018.

c. Notifica degli incidenti informatici secondo la Direttiva NIS

Il decreto di recepimento specifica che gli OSE dovranno inoltrare al CSIRT le notifiche di incidenti informatici con impatto rilevante sui servizi forniti.

Il decreto non fissa un limite temporale rigido per le notifiche, ma impone che le stesse vengano effettuate "senza ingiustificato ritardo". Tuttavia, le linee guida predisposte dalle autorità NIS nel 2019 definiscono in maniera più specifica la procedura da seguire per effettuare una notifica.

d. Direttiva NIS: Quadro sanzionatorio

La Direttiva NIS lascia agli Stati membri un margine di discrezionalità in merito alle sanzioni applicabili, a condizione che siano effettive, proporzionate e dissuasive. Nell'esercitare tale discrezionalità, il governo italiano ha stabilito che le autorità competenti possono applicare sanzioni amministrative fino a 150.000 euro in caso di violazione da parte degli operatori di servizi essenziali (o dei fornitori di servizi digitali) degli obblighi previsti dal decreto legislativo NIS.

[19] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf