

INDICE

1. INTRODUZIONE

2. LEGENDA

3. MISURE DI SICUREZZA

3.1. Postazioni di lavoro (PDL)

3.2. Reti (NET)

3.3. Data Center (DC)

3.4. Locali (LCL)

3.5. Accessi (ACC)

3.6. Processi (PRC)

3.7. Fornitori (SUP)

4. DOCUMENTI RICHIAMATI

REV n°0	Descrizione natura della modifica:			
Firma e Data	11/01/2024	11/01/2024	23/03/2024	
Nome	L. Perinati A. Boni F. Castelli L. Cagnoni G. Gattelli A. Tangenti Information Technology	Anna Giardini Director Information Technology	C. Maugeri Director L. Nicola CSR and Quality Assurance	L. Damiani Presidente Esecutivo
	Preparato	Controllato	Verificato	Approvato

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024
		Pagina 2 di 19

1. INTRODUZIONE

Il presente documento ha lo scopo di descrivere le misure tecniche di sicurezza informatica adottate a livello di asset infrastrutturali ICT (Information and Communication Technology), cioè di quelle componenti tecniche e organizzative gestite centralmente dall'IT nell'ambito dello sviluppo del sistema informativo.

Il documento è organizzato nel seguente modo:

Il capitolo **2. LEGENDA** contiene la descrizione degli acronimi utilizzati nel testo.

Il capitolo **3. MISURE DI SICUREZZA** descrive le misure di sicurezza di ciascun asset infrastrutturale.

Gli asset infrastrutturali sono suddivisi in:

1. **PdL**: postazioni di lavoro aziendali
2. **Reti**: reti dati locali a ciascuna sede, reti geografiche di interconnessione tra le sedi e rete Internet
3. **Data center**: infrastruttura hardware, software e di database centralizzata e comune agli applicativi del sistema informativo
4. **Locali**: locali centralizzati e di sede dedicati a contenere il data center e i vari dispositivi ICT
5. **Accessi**: meccanismi comuni a livello aziendale per la gestione degli accessi degli utenti alle postazioni di lavoro e agli applicativi del sistema informativo
6. **Processi**: procedure e istruzioni operative aziendali in ambito ICT
7. **Fornitori**: aziende specializzate che forniscono servizi di manutenzione e di supporto relativamente agli asset infrastrutturali e agli applicativi del sistema informativo

2. LEGENDA

Antivirus: programma che cerca ed elimina da un sistema le minacce software come i virus o altri software pericolosi per il funzionamento del sistema stesso (malware).

Antispam: programma che cerca ed elimina da un sistema lo spam cioè i messaggi o i contenuti web indesiderati, generalmente di tipo commerciale.

Antispyware: programma che cerca ed elimina da un sistema le minacce software come i “file spia” che tentano di carpire dati dal sistema stesso.

Firewall: dispositivo di sicurezza che, opportunamente configurato, consente di filtrare tutte le connessioni verso i dati e i servizi critici aziendali, abilitando solo il traffico consentito e implementando una difesa perimetrale della rete aziendale. È un dispositivo altamente critico che, in caso di guasto, può provocare l'impossibilità di accedere a dati e servizi informatici.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 3 di 19

IPS: Intrusion Prevention System, Sistema di Prevenzione delle Intrusioni dalla rete Internet alla rete aziendale da parte di utenti o programmi potenzialmente malevoli. È tipicamente abbinato a un sistema firewall. È un sistema più avanzato, complesso e costoso di un Intrusion Detection System (IDS) che, invece, segnala le intrusioni senza prevenirle.

LAN: Local Area Network, Rete Locale ad una sede.

MFA: Multi Factor Authentication o autenticazione a più fattori, tecnologia che permette di riconoscere una persona attraverso almeno due metodi di autenticazione (es. password più token inviato via SMS).

SIEM: Security Information and Event Management: servizio di analisi degli allarmi di sicurezza generati da applicazioni e da dispositivi di rete.

SOC: Security Operation Center: servizio di monitoraggio e intervento tecnico relativamente alla sicurezza informatica.

SIO: Sistema Informativo Ospedaliero.

SSO: Single Sign On, sistema di autenticazione che consente a un utente di autenticarsi una sola volta e di accedere a tutte le risorse informatiche a cui è abilitato.

VA-PT: Vulnerability Assessment – Penetration Test: servizio di valutazione delle vulnerabilità delle reti e dei sistemi informatici aziendali, anche tramite simulazioni di attacchi informatici.

VLAN: Virtual Local Area Network, Rete Dati Virtuale, porzione logica di LAN: consente di ottimizzare il traffico di rete e di limitare gli accessi ad aree non consentite; ciò aiuta ad esempio a contenere gli effetti di un'eventuale propagazione di virus sulla LAN ai soli computer appartenenti alla specifica VLAN; il traffico tra VLAN diverse viene filtrato da firewall.

VPN: Virtual Private Network; Rete Privata Virtuale, utilizzata per criptare i dati trasmessi su reti dati potenzialmente meno sicure (esempio reti pubbliche), per evitare che possano essere intercettati da terzi.

WAN: Wide Area Network, Rete Geografica, rete dati, fornita da un provider esterno, che collega tra loro le diverse sedi aziendali.

WLAN: Wireless Local Area Network, Rete Locale wireless, con trasmissione dei dati via etere anziché via cavo. La comunicazione effettuata sulle WLAN è particolarmente esposta al rischio di intercettazione da parte di utenti dotati di postazioni portatili, anche da zone esterne e limitrofe all'azienda.

Web Content Filtering: sistema di protezione contro i siti web pericolosi (che possono cioè danneggiare le postazioni di lavoro poiché contengono malware); può essere utilizzato anche per impedire l'accesso a siti che non sono di interesse aziendale e a siti che forniscono servizi che possono occupare la linea Internet a danno degli altri utenti (soprattutto per le sedi periferiche).

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 4 di 19

3. MISURE DI SICUREZZA

3.1. Postazioni di lavoro (PDL)

PDL01 – Tipologia e utilizzo delle PdL

Le PdL utilizzate in azienda sono dei seguenti tipi:

- PC con sistema operativo Microsoft Windows 10 e Windows 8.1;
- Notebook con sistema operativo Microsoft Windows 10;
- PC carrellati con sistema operativo Microsoft Windows 10, utilizzati dal personale di reparto per la cartella clinica al letto del paziente;
- Smartphone aziendali con sistema operativo Android, utilizzati dal personale di reparto per il diario clinico in mobilità;
- Tablet aziendali, utilizzati dal personale di reparto per il sistema Access Manager.

PDL02 – Installazione delle PdL

Installazione e immagini

Le PdL vengono create a partire da installazioni standard (immagini) che contengono i software utilizzabili per quella specifica tipologia di PdL.

Le PdL danneggiate vengono ripristinate a partire dalle immagini utilizzate per la loro creazione iniziale.

Le immagini sono conservate su una workstation dedicata, a cui ha accesso esclusivamente il personale del fornitore incaricato dell'installazione delle PdL che opera on-site presso ICSM.

Una copia delle immagini viene tenuta presso la sede del fornitore incaricato delle installazioni delle PdL, per consentire il roll-out in tutte le sedi aziendali.

Le modifiche alle immagini e ai relativi software vengono decisi in riunioni congiunte tra fornitore e IT.

Customizzazione

Successivamente all'installazione dell'immagine sulla PdL vengono effettuate le seguenti attività di configurazione da parte del fornitore incaricato:

1. installazione di eventuali software aggiuntivi (se autorizzati e licenziati)
2. connessione della PdL al dominio aziendale
3. assegnazione alla PdL di un nome macchina e di un indirizzo IP valido (fornito dall'IT); nel caso la PdL sostituisca una PdL guasta o in dismissione, il nome macchina e l'indirizzo IP rimangono gli stessi.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 5 di 19

Al momento della consegna all'utente vengono effettuate le ulteriori attività di personalizzazione:

1. configurazione di periferiche specifiche (esempio: stampanti, lettori di smartcard)
2. travaso di dati dalla vecchia alla nuova PdL
3. installazione di lettore smartcard SISS, se previsto
4. consegna all'utente, verifica di funzionamento e accessibilità da parte dell'utente
5. smaltimento dischi della vecchia PdL

PDL03 – Dismissione delle PdL e dei dischi

Il fornitore si occupa del ritiro e dello smaltimento secondo la normativa vigente di tutte le PdL e delle parti dismesse o sostituite, facenti parte del perimetro della fornitura.

Si occupa inoltre di rendere illeggibili tutti i dischi dati, tramite formattazione a basso livello, prima dello smaltimento degli stessi.

PDL04 – Autenticazione alle PdL

Le PdL aziendali sono connesse al dominio aziendale (vedi *ACC01 – Domain controller aziendale*).

Sono pertanto accessibili esclusivamente da utenti registrati e attivi sul dominio aziendale e previa autenticazione informatica tramite login e password.

Le PdL condivise da più utenti sono utilizzate da ciascun utente con le proprie credenziali personali.

Unica eccezione è costituita dai PC carrellati ai quali si può accedere tramite un'utenza generica (l'accesso ai servizi applicativi è in ogni caso possibile solo tramite autenticazione informatica personale (login e password)).

PDL05 – Antivirus e antispyware

Sulle PdL in dominio con sistema operativo Windows, sono attivi i software antivirus e antispyware Sophos.

L'aggiornamento del database delle impronte dei virus è automatico e ha frequenza giornaliera.

L'aggiornamento del motore dell'antivirus viene effettuato automaticamente al rilascio di una nuova versione del motore.

Il sistema Sophos è in cloud. L'accesso alla console avviene tramite MFA.

PDL06 – Screensaver

Sulle PdL in dominio con sistema operativo Windows, a eccezione dei PC carrellati, è implementata la funzionalità che attiva uno screensaver protetto da password che blocca automaticamente la sessione dell'utente dopo un timeout di 30'.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 6 di 19

PDL07 – Amministrazione remota delle PdL

Le PdL in dominio con sistema operativo Windows sono dotate di un software di controllo remoto (Ultra VNC) utilizzabile dagli operatori incaricati dell'helpdesk (fornitore esterno e IT).

Il software è configurato in modo tale che l'utente debba dare un'autorizzazione esplicita per consentire la connessione remota da parte di un operatore di helpdesk.

Sulle PdL è installato il solo modulo server. Non è invece presente il modulo client del VNC.

La comunicazione tra moduli server e viewer del VNC è cifrata.

PDL08 – Inventario dell'hardware e del software delle PdL

LANsweeper è lo strumento di asset inventory aziendale, utilizzato dal fornitore incaricato della gestione delle PdL per effettuare il censimento automatico delle configurazioni hardware e software delle PdL attive, necessario per svolgere le attività di manutenzione e di supporto tecnico.

PDL09 – Patch di sicurezza sulle PdL

Tutte le PdL in dominio con sistema operativo Windows, scaricano automaticamente, ogni settimana, le ultime patch di sicurezza di sistema operativo, accedendo al servizio Windows Update online di Microsoft. Quindi il sistema notifica all'utente che è disponibile un aggiornamento che diventerà attivo con il primo riavvio del PC.

PDL10 – Dati locali sulle PdL

L'archiviazione di dati non anonimizzati sulle PdL è deprecata, come indicato nelle linee guida sulla sicurezza informatica aziendali (vedi IO ICSM LGSI Linee guida sulla sicurezza informatica).

I dati di tipo personale e/o sensibili devono essere trattati tramite gli applicativi del sistema informativo.

Per quanto riguarda gli smartphone utilizzati per l'inserimento in mobilità delle note di diario clinico del paziente, l'applicativo è stato sviluppato in modo tale che sul dispositivo non rimanga memorizzato nessun dato o immagine relativa al paziente.

PDL11 – Protezione dei notebook aziendali

Tutti i notebook aziendali sono dotati delle seguenti misure di sicurezza:

- disco cifrato (tramite Sophos / Bitlocker);
- sincronizzazione automatica su OneDrive personale dell'utente, delle cartelle Documenti, Immagini e Desktop presenti sul notebook;

L'utente dotato di notebook aziendale si collega alla rete aziendale utilizzando un VPN client, inserendo la propria credenziale di Active Directory e un secondo fattore ricevuto via email.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 7 di 19

3.2. Reti (NET)

NET01 – Struttura della rete

La rete dati di ICSM comprende:

1. la rete geografica (WAN) che connette tutte le sedi,
2. le reti locali (LAN) di ciascuna sede,
3. la zona demilitarizzata (DMZ)
4. la rete Internet

WAN

La WAN si basa sulla rete MPLS di TIM.

La WAN connette tutte le sedi aziendali e ha come centro stella la sede di Pavia via Maugeri.

Le varie sedi sono connesse alla WAN prevalentemente in fibra ottica.

LAN

Il cablaggio delle LAN delle diverse sedi è in categoria 5e o successiva.

Gli switch, del produttore Cisco, sono di tipologia professionale, gestibile da remoto.

In tutte le sedi la LAN è strutturata in VLAN.

Le principali VLAN sono quelle degli applicativi del sistema informativo, quella del data center locale alla sede, quella della rete Wifi, quella della telefonia VoIP, quella del Servizio di Diagnostica per Immagini, più altre VLAN di servizio o relative a servizi specifici di sede.

Nel centro stella, per ciascun data center, le principali VLAN sono quella interna al data center, che comprende tutti i servizi critici aziendali e quella della DMZ.

DMZ

La DMZ è implementata in cloud Azure di Microsoft e viene utilizzata per esporre su Internet servizi applicativi on-premise, tramite l'implementazione di reverse proxy.

La connessione tra il data center aziendale e il cloud Microsoft è realizzata tramite una VPN su Internet.

Internet

La rete Internet aziendale è la rete GARR (Rete Dati del MIUR per gli IRCCS) a 1000 Mbps, con linea di backup a 100 Mbps.

Il servizio aziendale di accesso a Internet viene fornito da un proxy centralizzato, situato nel data center di Pavia e utilizzato da tutti gli utenti di ICSM, inclusi quelli delle sedi remote.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 8 di 19

NET02 – Ridondanza della rete

WAN

In tutte le sedi la connessione alla MPLS è costituita da una linea principale e da una linea di backup.

Nel centro stella le linee primaria e di backup si attestano, internamente, sui 2 locali di data center attraverso 2 percorsi separati e indipendenti.

In tutte le sedi i router di connessione alla WAN (uno per la linea principale e uno per quella di backup) sono connessi ai due firewall di sede (primario e backup) tramite doppi switch e doppi percorsi.

Nel corso del 2024 si prevede di realizzare una o più SD-WAN per le sedi che si doteranno di connettività Internet adeguata.

LAN

In tutte le sedi gli apparati di distribuzione della rete e i controller wifi sono ridondati.

Nell'istituto di Pavia sono ridondate le linee di connessione di ciascuna base torre con ciascuno dei due locali di data center.

DMZ

La ridondanza di connettività tra la parte di DMZ implementata in Azure e i data center aziendali si basa su quella della rete Internet.

Internet

L'accesso alla rete Internet è realizzato con doppia linea in fibra ottica (principale e backup) con percorsi separati e indipendenti per ciascun locale di data center.

I server proxy sono virtualizzati su infrastruttura VMWare (vedi Data Center).

Firewall

Sia i firewall centrali che quelli di sede periferica sono doppi e clusterizzati.

NET03 – Capacità della rete

WAN

Le linee primarie sono dimensionate a 100 Mbps, ad eccezione delle sedi in Sicilia e a Padova che hanno una banda di 20 Mbps.

Il centro stella ha una banda di 1000 Mbps

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 9 di 19

LAN

Gli apparati di rete sono dimensionati in funzione del numero di PdL gestite e sono di tipo professionale.

Firewall

Sia i firewall centrali che quelli di sede periferica sono dimensionati in funzione del numero di accessi gestiti.

NET04 – Autenticazione agli apparati di rete

Gli apparati di rete sono connessi al dominio aziendale (vedi *ACC01 – Domain controller aziendale*).

Sono pertanto accessibili esclusivamente da utenti registrati e attivi sul dominio aziendale e previa autenticazione informatica tramite login e password.

Le credenziali di accesso sono fornite ai soli tecnici incaricati delle attività di manutenzione e controllo.

NET05 – Firewall

In ICSM sono presenti complessivamente 38 firewall: 4 firewall sono dedicati alla protezione del data center aziendale e 2 a salvaguardia di ciascuna sede.

I firewall vengono configurati dal personale tecnico dell'IT, al fine di regolare in modo mirato gli accessi degli utenti alle risorse informatiche.

Il criterio utilizzato è quello della pertinenza degli accessi: a gruppi di utenti, identificati in base al ruolo, viene consentito l'accesso ai servizi informatici di competenza.

I firewall utilizzati sono del produttore Fortinet.

NET06 – Crittografia sulle reti

Tutta la comunicazione effettuata sulle reti Wifi è cifrata.

Tutte le connessioni tra i fornitori e i sistemi applicativi di competenza presenti nel data center aziendale sono effettuate tramite Internet e cifrate tramite VPN di tipo Client-to-LAN o, con i fornitori maggiori, di tipo LAN-to-LAN.

Le modalità per richiedere l'attivazione di una VPN per l'accesso remoto di un fornitore sono descritte nella IO ICSM GCI **Gestione credenziali informatiche**.

A tutti i fornitori di sistemi applicativi con interfaccia web viene richiesto di utilizzare esclusivamente il protocollo https.

Tutta la restante comunicazione sulle LAN di ICSM viene effettuata in modalità non cifrata.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 10 di 19

NET07 – Indirizzamento IP

L'indirizzamento IP aziendale è statico su classi di indirizzamento private.

Non sono presenti server DHCP sulla rete aziendale, ad eccezione di quelli dedicati ai servizi di rete VoIP, di rete Citrix e di rete Guest che sono segregati su VLAN dedicate.

NET08 — Antivirus e antispam

Posta elettronica

È attivo un sistema antivirus / antispam di Microsoft integrato in Exchange365.

Navigazione Internet

È attivo, centralmente presso il data center, un sistema di antivirus di Forcepoint, che controlla la navigazione Internet effettuata da qualunque postazione di lavoro connessa alla rete dati di ICSM.

L'aggiornamento del database delle impronte dei virus è automatico e in maniera continuativa.

NET09 — Filtraggio dei contenuti Internet

È attivo, centralmente presso il data center, un sistema di filtraggio dei contenuti di Forcepoint, che controlla la navigazione Internet effettuata da qualunque postazione di lavoro connessa alla rete dati di ICSM.

Il filtraggio dei contenuti viene realizzato sulla base di categorie di siti abilitate o disabilitate e la configurazione viene effettuata dall'IT.

Per alcune postazioni dell'Alta Direzione e di alcuni servizi che svolgono attività istituzionali (esempio Servizio CNIT dell'Istituto di Pavia), pur rimanendo in essere tutte le protezioni sulla navigazione Internet, è limitato o disattivato il filtraggio dei contenuti.

NET10 – Reverse proxy / web application firewall (WAF)

A tutti i fornitori di sistemi applicativi che debbano esporre su Internet servizi applicativi erogati on-premise viene richiesto di utilizzare un reverse proxy / web application firewall.

Nel caso il fornitore non riesca a garantire autonomamente questo servizio, ICSM consente al fornitore di appoggiarsi alla propria infrastruttura in cloud Azure di Microsoft che utilizza un WAF Palo Alto.

Per il sito web aziendale, gestito in hosting dal fornitore NoHup, è stato implementato un WAF aggiuntivo al firewall di base già presente a protezione del sito.

NET11 — Postazioni Internet per navigazione libera

È consentito a ciascun Istituto di dotarsi di postazioni dedicate alla navigazione libera.

Tali postazioni sono connesse direttamente a Internet e sono separate, per motivi di sicurezza, dalla rete locale di ICSM.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 11 di 19

NET12 — Wifi per navigazione libera

L'Istituto di Pavia via Maugeri (alcune aree) e la sede dell'Amministrazione Centrale sono coperte da un servizio di accesso libero a Internet tramite la rete wifi aziendale.

Il Captive Portal utilizzato è Cisco ISE, che rilascia credenziali a tempo agli utenti che si registrano sul portale.

Nel corso del 2024 è prevista la dotazione di un sistema di Captive Portal in cloud, integrato con le reti wifi di istituto, per la navigazione libera degli utenti tramite wifi.

Ciascun Istituto che vorrà utilizzare questo servizio dovrà dotarsi di una linea Internet locale.

NET13 — Servizi di sicurezza

Nel corso del 2024, anche in funzione della disponibilità del budget, sarà valutata l'attivazione di servizi di sicurezza quali SIEM, VA-PT e SOC.

3.3. Data Center (DC)

DC01 – Data Center centrale

In ICSM è presente un data center (DC), costituito da due locali posizionati nella sede di Pavia Cravino, che contiene gli asset infrastrutturali comuni a diversi sistemi applicativi.

Il DC è costituito da una Storage Area Network (SAN) e da un'infrastruttura di server fisici e virtuali.

La SAN è realizzata da una rete ad alta velocità (Gigabit/s in fibra e rame) e da dispositivi di memorizzazione di massa (storage) condivisi e utilizzabili da qualunque server della SAN.

I database Oracle aziendali sono consolidati su un cluster di server fisici.

La licenza Oracle è quella Standard, le release sono la 11.x e la 12.x.

I database Informix sono installati su un cluster di server fisici.

La licenza Informix è quella Standard, la release è la 14.x.

Tutti gli altri server sono implementati su un'infrastruttura virtuale VMWare Enterprise 7.x basata su 6 server fisici.

DC02 – Dotazioni ICT di sede

In ciascuna sede è presente un locale tecnico dedicato a contenere i firewall di sede e i router della rete geografica.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 12 di 19

DC03 – Business continuity

Tra i principali criteri utilizzati nella progettazione dell'infrastruttura informatica del data center vi è quello relativo all'eliminazione dei single point of failure, che viene perseguito tramite la ridondanza delle componenti hardware e delle connessioni tra ciascun dispositivo.

Gli **storage** della SAN sono in configurazione RAID 6.

I **server di database** Oracle e Informix sono clusterizzati e dotati di componenti hardware duplicate (schede di rete, alimentatori, dischi di sistema operativo ...).

I **server virtuali** condividono un'infrastruttura ridondata di 6 server fisici dotati di componenti hardware duplicate (schede di rete, alimentatori, dischi di sistema operativo ...).

Tutti gli **apparati di rete** del data center sono duplicati, così come le connessioni tra qualunque dispositivo sono doppie su percorsi indipendenti, ove tecnologicamente supportato.

Relativamente ai **firewall** presenti nel DC vedi *Firewall*.

DC04 – Backup e restore

I backup dei **database** vengono realizzati tramite gli strumenti specifici di ciascun DBMS (es. RMAN) e poi salvati sugli storage di data center tramite il sistema CommVault.

Il backup dei **server virtuali** (dati e configurazioni) vengono effettuati tramite Veeam e poi salvati sugli storage di data center.

I backup hanno frequenza giornaliera e possono essere di varia tipologia (completo, incrementale, differenziale) e con diversa retention (settimanale, mensile, annuale).

Gli esiti dei backup vengono verificati giornalmente dal personale incaricato dell'IT, secondo la procedura IO ICSM GB **Gestione backup**.

I sistemi applicativi installati presso il DC, prima dell'avviamento in produzione, vengono configurati per poter sfruttare l'infrastruttura di backup aziendale.

Nel corso del 2024, anche in funzione della disponibilità del budget, sarà valutata l'attivazione di un servizio di golden backup.

Relativamente al restore dei dati, le modalità di restore vengono definite e testate dall'IT, assieme ai fornitori dei diversi sistemi informatici, al momento dell'attivazione di un nuovo sistema.

I test di restore vengono effettuati durante le attività di manutenzione straordinaria dei sistemi.

DC05 – Disaster recovery

In ICSM è stata realizzata una soluzione di DR di campus basata sulla presenza di due locali, separati e sufficientemente distanti tra loro (circa 150 m), connessi da una linea dati ad alta velocità, nei quali è stata distribuita l'infrastruttura di alta affidabilità (storage e server) già presente nel precedente locale di data center (vedi *Business Continuity*).

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 13 di 19

Uno storage della SAN è stato posizionato nel primo locale, mentre il secondo storage, gemello del primo, è stato posizionato nel secondo locale.

I due storage sono tra loro connessi in fibra ottica in configurazione attivo-attivo.

Così i cluster di database server Oracle e Informix sono stati sdoppiati posizionando un server nel primo locale e uno nel secondo. Tutti i server sono in configurazione attiva.

I server dell'infrastruttura virtuale VMWare sono stati suddivisi tra i due locali: tre server in un locale e tre nell'altro.

DC06 – Crittografia dei dati sugli storage

Le unità storage della SAN non implementano la cifratura dei dati (crittografia at rest).

DC07 – Autenticazione agli apparati di data center

Le credenziali primitive (administrator, root, ...) degli asset infrastrutturali del data center non vengono utilizzate per le normali attività di gestione e manutenzione dei sistemi, ma vengono custodite dai sistemisti dell'IT.

I sistemisti dell'IT dispongono di credenziali nominative e personali per accedere ai sistemi informatici di competenza.

Ai fornitori viene assegnata una credenziale per accedere ai sistemi informatici di competenza ed è compito del fornitore il tenere traccia dei tecnici che operano con tale credenziale.

I criteri e le modalità per gestire le credenziali di accesso degli amministratori di sistema sono contenuti nella IO ICSM ADS **Gestione amministratori di sistema**.

Nel budget 2024 è stata prevista l'acquisizione di una PAM.

3.4. Locali (LCL)

LCL01 – Tipologia

I locali contenenti le apparecchiature che costituiscono l'infrastruttura informatica sono:

- i 2 locali di data center localizzati nell'istituto di Pavia via Maugeri
- i locali tecnici presenti nelle sedi aziendali periferiche

LCL02 – Accessi ai locali di data center

L'accesso ai due data center è limitato al personale dell'area sistemistica dell'IT.

I fornitori che devono accedere ai data center vengono affiancati dal personale dell'area sistemistica dell'IT per tutto il tempo di permanenza nei locali.

	LINEA GUIDA ICSM	LG ICSM MSIN-0
	MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	Data: 11/01/2024 Pagina 14 di 19

I locali di data center sono tenuti chiusi a chiave e sono dotati di un sistema antintrusione volumetrico, attivabile / disattivabile tramite badge personale e dotato di segnalazione di allarme al centralino della sede di Pavia via Maugeri.

Le chiavi e il badge di accesso ai locali sono in possesso del personale dell'area sistemistica dell'IT e del servizio di manutenzione degli impianti della sede di Pavia via Maugeri.

LCL03 – Sistemi complementari di data center

Il data center primario è dotato di:

- doppia linea di alimentazione verso due gruppi di continuità separati ed autonomi,
- sistema di climatizzazione su 2 apparati indipendenti,
- rilevatore fumi e antincendio con spegnimento a saturazione,
 - sensore di umidità sotto il pavimento flottante,
 - rinforzo dei muri in cartongesso,
 - porta di accesso al locale rinforzata,
 - protezione da infiltrazioni di acqua piovana.

Il data center secondario è dotato di:

- doppia linea di alimentazione verso due gruppi di continuità separati ed autonomi,
- sistema di climatizzazione su 2 apparati indipendenti; questo sistema è stato rinnovato nel corso del 2020 e reso simile a quello del CED primario,
- rilevatore fumi e antincendio con spegnimento a saturazione,
 - videocamere c/c con monitor al centralino del centro medico.

LCL04 – Accessi ai locali tecnici di sede

I dispositivi di rete, i firewall e i file-server presenti nelle sedi di ICSM, sono dislocati in locali tecnici multifunzione.

L'accesso a tali locali è condiviso tra il personale dell'IT, il personale di assistenza informatica e il personale di sede addetto alla manutenzione degli impianti.

Nei rari casi in cui i dispositivi di rete sono inseriti in zone aperte al pubblico, sono contenuti in armadi chiusi a chiave.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 15 di 19

3.5. Accessi (ACC)

ACC01 – Domain controller aziendale

ICSM è dotata di un sistema ActiveDirectory aziendale di Microsoft, che contiene l'anagrafica unica e centralizzata degli utenti aziendali dei sistemi informatici aziendali.

ACC02 – Ridondanza del domain controller aziendale

Il domain controller aziendale è clusterizzato nel Data Center e replicato sui file-server di 2 sedi aziendali e una istanza è tenuta in cloud Azure.

ACC03 – Gestione delle password

Relativamente alla gestione delle password, il sistema ActiveDirectory implementa le seguenti funzionalità:

1. credenziali nominative e basate su login e password
2. le credenziali vengono disattivate ma mai eliminate
3. cripting one-way delle password
4. obbligo di cambio password alla prima connessione
5. scadenza della password dopo 3 mesi
6. lunghezza minima della password di 8 caratteri
7. la password deve soddisfare almeno tre dei seguenti requisiti: (1) contenere almeno un carattere maiuscolo (A-Z), (2) contenere almeno un carattere minuscolo (a-z), (3) contenere un numero (0-9) e (4) contenere un simbolo (!?@\$&, ecc.)
8. la password non può contenere più di due caratteri consecutivi del nome completo o dell'account dell'utente
9. impossibilità di riutilizzare una delle ultime 3 password precedentemente utilizzate
10. impossibilità di cambiare la password prima di 24 ore
11. possibilità dell'utente di cambiare la password in qualunque momento, anche indipendentemente dalla scadenza temporale della stessa.

ACC04 – Autenticazione applicativa

I sistemi applicativi possono integrarsi con il domain controller aziendale per sfruttarne il meccanismo di autenticazione informatica.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 16 di 19

ACC05 – Autorizzazione applicativa

L'autorizzazione degli utenti all'accesso agli applicativi, normalmente basata sulla profilazione dei ruoli, viene normalmente effettuata dai sistemi applicativi secondo proprie modalità interne.

I sistemi applicativi che lo prevedano possono integrarsi ed utilizzare il domain controller aziendale anche per l'autorizzazione applicativa.

ACC06 – Tentativi di connessione

Il sistema Active Directory è configurato in modo tale che, dopo 40 tentativi di autenticazione effettuati entro un periodo di 10 minuti, la credenziale dell'utente viene temporaneamente bloccata per 15 minuti.

ACC07 – Log degli accessi degli amministratori di sistema

Non è al momento attivo un log agli accessi degli amministratori di sistema (Provvedimento del Garante Privacy del 27.11.2008).

Poiché per implementare questa funzionalità è necessario realizzare preventivamente un sistema di raccolta dei log degli accessi degli AdS sui diversi sistemi IT presenti nel data center (server Windows, server Linux, database Oracle, firewall, ecc.), questo progetto è stato previsto nell'ambito del budget 2024 in corso di approvazione.

ACC08 – Multi Factor Authentication

Tutti gli utenti che utilizzano servizi aziendali in cloud per i quali è attivo un SSO-SingleSignOn (cioè le credenziali di autenticazione sono gestite dal Domain Controller aziendale), quando si collegano dall'esterno della rete ICSM devono utilizzare la Multi Factor Authentication.

Un esempio è il servizio di posta elettronica.

ICSM dispone del servizio di Multi Factor Authentication di Microsoft, utilizzabile dagli utenti tramite la app Microsoft Authenticator installata sul cellulare personale.

3.6. Processi (PRC)

PRC01 – Istruzioni operative

Le procedure aziendali in ambito informatico sono le seguenti:

1. IO ICSM LGS **Linee guida sulla sicurezza informatica** (vedi PRC02 – Linee Guida sulla Sicurezza Informatica)
2. IO ICSM GCI **Gestione delle credenziali informatiche**: descrive le modalità per la gestione delle credenziali di accesso alle PdL, agli applicativi clinico-sanitari e amministrativi e ai servizi Internet (posta elettronica e navigazione) da parte degli utenti aziendali

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 17 di 19

3. IO ICSM HD Help desk informatico: descrive le modalità operative per interagire con il servizio di service desk aziendale e per la gestione delle chiamate di supporto da parte degli utenti aziendali
4. IO ICSM ADS Gestione amministratori di sistema: definisce le regole per la gestione degli amministratori di sistema e più in generale delle figure professionali, sia interne che esterne all'azienda, che si occupano della gestione e della manutenzione dei sistemi informatici in perimetro o di sue componenti
5. IO ICSM GB **Gestione backup**: descrive le modalità organizzative generali utilizzate dall'IT per la gestione dei backup dei sistemi informatici ospitati nel data center aziendale e dei file-server di istituto

PRC02 – Linee Guida sulla Sicurezza Informatica

È regolato dalla procedura IO ICSM LGSI **Linee Guida sulla Sicurezza Informatica**.

Il documento ha lo scopo di contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano causare problemi o minacce alla sicurezza nel trattamento dei dati.

Le linee guida disciplinano le condizioni per il corretto utilizzo degli strumenti informatici da parte degli utilizzatori e forniscono informazioni utili per comprendere cosa può fare ogni utilizzatore per contribuire alla sicurezza informatica aziendale.

Gli ambiti coperti dalle linee guida sono:

1. utilizzo del Personal Computer
2. utilizzo della rete aziendale
3. gestione delle credenziali e delle password
4. utilizzo della posta elettronica
5. utilizzo di Internet
6. protezione da virus informatici

La procedura viene rivista ogni 3 anni, come previsto dal sistema qualità aziendale, e in tutti i casi in cui siano richieste delle modifiche a seguito di cambiamenti tecnologici e/o organizzativi.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 18 di 19

3.7. Fornitori (SUP)

Sono attivi contratti di supporto, di manutenzione e di monitoraggio dei sistemi con tutti i fornitori di asset informatici.

SUP01 – Area tecnologica IT

L'IT comprende nel proprio organigramma una sezione denominata Area Tecnologica formata da 5 sistemisti dedicati alla progettazione, manutenzione e gestione degli asset infrastrutturali.

SUP02 – Monitoraggio e supporto specialistico del data center

È attivo con il fornitore Lutech un contratto 24x7 per il monitoraggio sistemistico dei sistemi installati presso il data center e per il supporto tecnico specialistico, sia remoto che on-site, in caso di problemi hardware o software su tali sistemi.

L'attività di monitoraggio viene svolta in modo automatico tramite sonde software che controllano continuamente i sistemi e generano allarmi quando necessario, inviando segnalazioni sia all'IT che al fornitore stesso.

SUP03 – Monitoraggio e supporto specialistico dei database

Database Oracle

È attivo con il fornitore Lutech un contratto di manutenzione e di monitoraggio 24x7 di tutte le istanze Oracle installate sui database server aziendali (vedi **Infrastruttura Data Center**).

Database Informix

Non è attivo alcun contratto di supporto tecnico avanzato per le basi dati del SIO clinico sviluppato internamente. (Fino al 2021 è stato attivo un contratto con il fornitore TeeTech).

È invece attivo un regolare contratto di manutenzione software per il database Informix.

Database SAP

È attivo con il fornitore TechWall un contratto di supporto, manutenzione e monitoraggio 24x7 delle istanze SAP.

In aggiunta ai contratti di base, la gestione, la manutenzione, il supporto e il monitoraggio di ciascun database applicativo sono regolati da specifici contratti con i fornitori dei diversi applicativi.

	LINEA GUIDA ICSM MISURE DI SICUREZZA DELL'INFRASTRUTTURA ICT	LG ICSM MSIN-0
		Data: 11/01/2024 Pagina 19 di 19

SUP04 – Monitoraggio e supporto specialistico delle reti

Reti locali

È attivo con il fornitore Lutech un contratto di manutenzione degli apparati di rete e di supporto tecnico relativamente alla LAN aziendale di tutte le sedi.

È inoltre attivo un servizio 24x7 di monitoraggio delle LAN aziendali, che prevede la segnalazione automatica, sia all'IT che al NOC del fornitore stesso, degli eventi critici che si verificano sugli apparati di rete.

L'intervento on-site è previsto con lo stesso fornitore in modalità 9x5.

Rete geografica

La rete geografica è gestita da TIM e il contratto di fornitura prevede livelli di servizio definiti.

Rete Internet

È attivo un servizio 12x5 di assistenza e manutenzione della rete GARR erogato dal GARR-NOC.

SUP05 – Monitoraggio e supporto specialistico dei firewall

È attivo con il fornitore WellComm, un servizio 24x7 di monitoraggio dei firewall e delle VPN, che prevede la segnalazione di guasti e malfunzionamenti all'IT e al NOC del fornitore stesso e, ove possibile, l'intervento da remoto del fornitore per la risoluzione dei problemi.

SUP06 – Fornitura, manutenzione e supporto delle PdL

È attivo con il fornitore BCS un contratto pluriennale che prevede la fornitura di PC a noleggio, comprensivo di manutenzione hardware delle PdL, inclusa la gestione delle PdL SISS, e di un servizio di helpdesk informatico attivo h24.

4 DOCUMENTI RICHIAMATI

IO ICSM LGSI Linee guida sulla sicurezza informatica

IO ICSM GCI Gestione delle credenziali informatiche

IO ICSM HD Help desk informatico

IO ICSM ADS Gestione amministratori di sistema

IO ICSM GB Gestione backup