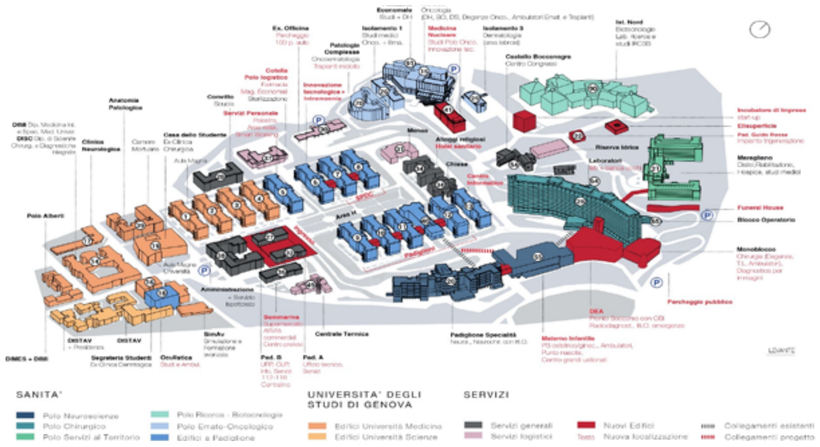
Cybersecurity e disponibilita’ dei servizi sanitari in un ecosistema digitale avanzato



IL POLICLINICO: UN'AZIENDA COMPLESSA

Una città nella città (12 km di viali interni e un territorio di circa 35 ettari, conformazione a padiglioni)

Polo di riferimento per tutta la Liguria, IRCCS con riconoscimento nella disciplina di Oncologia e Neuroscienze

Funzioni istituzionali di didattica e di ricerca dell'Università degli Studi di Genova

Un elevato numero di device

PDL (pc, stampanti telefoni)

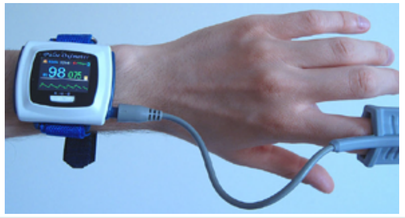
Sistemi centrali (server, storage, firewall)

Sistemi periferici (telecamere, lettori badge, sistemi di apertura porte, citofoni, eliminacode, dispositivi termoelettrici e ambientali, frigoriferi…..)

Dispositivi di rete (router, switch, access point)

Dispositivi medici

1354 apparecchiature collaudate nel 2022



...connessi in rete

Progettazione e posa dei percorsi in fibra ottica tra i padiglioni

Gestione di un elevato numero di apparati di rete

Gestione di device appartenenti a diversi enti e servizi, non solo ospedalieri

IRCCS - UNIGE - IIT - ASL3
NUE 112 - 118 LIGURIA

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Perché garantire la connettività di tutti questi device?

La quasi totalità dei servizi ospedalieri è oggi supportata dalle tecnologie informatiche e di telecomunicazione

- Sistema Informativo Ospedaliero SIO
  2500 utenti
- Sistema informativo Radiologico e cardiologico RIS-CIS/PACS
  800 utenti
- Sistema Informativo di Laboratorio LIS per accessi esterni
  940 utenti
- Centro Trasfusionale Ospedaliero
  160 utenti
- Software regionale di raccolta sangue
  65 utenti
- Registro di Blocco Operatorio
  300 utenti

QUAL È IL RUOLO DEI DISPOSITIVI MEDICI NEI SISTEMI IT?

Strumenti destinati dal fabbricante ad essere impiegati sull'uomo per destinazioni d'uso mediche specifiche quali la diagnosi, prevenzione, monitoraggio, trattamento, ecc. (Regolamento UE 2017/745)

Prelevano, quindi, segnali dall'uomo e li inviano ai sistemi IT, per essere elaborati e gestiti

I DISPOSITIVI MEDICI SONO DEVICE

CONNESSI IN RETE

QUALI RISCHI IN UN SISTEMA COSÌ COMPLESSO

Attacco informatico o cyber-attacco

- **da individui o da organizzazioni esterne**
- **ai sistemi informatici**, alle infrastrutture, alle reti di calcolatori e/o dispositivi elettronici di sistemi critici
- tramite **atti malevoli, finalizzati al furto, alterazione e/o distruzione di specifici obiettivi**

I dispositivi medici rappresentano uno dei principali bersagli di un cyber attacco

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Quali conseguenze

Non riuscire a garantire la continuità operativa del sistema

- Perdita di dati
- Impossibilità di accesso ai sistemi
- Assenza di integrazione tra i dispositivi medici e i sistemi centrali
- Procedure di emergenza

laboratorio SANITÀ 2030
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

COME PREVENIRE

Individuare le **vulnerabilità** del sistema e adottare le giuste **misure di sicurezza** per eliminarle o ridurle

- Acquisire le **competenze** necessarie
- Adottare **misure di sicurezza tecniche**
- Adottare **misure di sicurezza organizzative**

RENDERE CONSAPEVOLI

Pillole di cybersecurity

Campagne di phishing

ACQUISIRE COMPETENZE

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

MISURE TECNICHE

- Segmentazione della rete (VLAN) e FIREWALL perimetrale
- Predisporre un INVENTARIO DEI DEVICE connessi in rete e dei SOFTWARE AUTORIZZATI
- Adottare CONFIGURAZIONI STANDARD dei device
- Installare periodicamente gli AGGIORNAMENTI DI SICUREZZA sui device
- Archiviare i dati in sistemi centrali, gestiti dal servizio IT, che esegue periodiche COPIE DI SICUREZZA
- Non adottare utenze di accesso generiche, ma adottare UTENZE NOMINALI e non con ruolo di amministratore
- Raccolta LOG AMMINISTRATORI di sistema
- Installare ANTIVIRUS e/o sistemi XDR (eXtended Detection and Response)

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Normativa di riferimento

UE/2016/1148 Direttiva NIS
Network and Information Security
recepita in Italia con D. Lgs. n. 65/2018

considera gli Istituti Sanitari (compresi Ospedali e cliniche private) **Operatori di Servizi Essenziali (OSE)** per i quali è necessario adottare misure di sicurezza volte alla realizzazione di un ambiente digitale sicuro e affidabile

prevede il rispetto di obblighi da parte degli OSE e dei fornitori di servizi digitali relativamente all'**adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante**

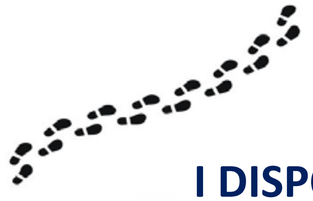
l'**Agenzia per la Cybersicurezza Nazionale (ACN)** è autorità nazionale competente NIS e vigila sull'applicazione del D.L. 65/2018 a livello nazionale, esercitando altresì le relative funzioni ispettive e sanzionatorie

Collaborazione tra IC e IT:

- Stesura del Capitolato Tecnico
- Valutazione delle offerte
- Installazione del DM

Collaudare quando il DM:

- è correttamente integrato con i sistemi aziendali
- rispetta lo standard aziendale di connessione in rete
- rispetta le misure di sicurezza



I DISPOSITIVI MEDICI: GESTIRE IL CAMBIAMENTO

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Grazie per l'attenzione

#sanita2030
www.sanita2030.it

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio