



SIMPOSIO AFI

65° SIMPOSIO AFI **L'Industria della Salute** **nel tempo dell'Intelligenza** **Artificiale**

Rimini, 10/12 Giugno 2026

Multi-Compliance NIS2/GxP come leva
strategica e sostenibile per la conformità
alle nuove normative europee di
Cybersecurity

Giuseppe Bungaro – Adeodata Srl





Giuseppe Bungaro

Head of Digital Transformation – Adeodata SA

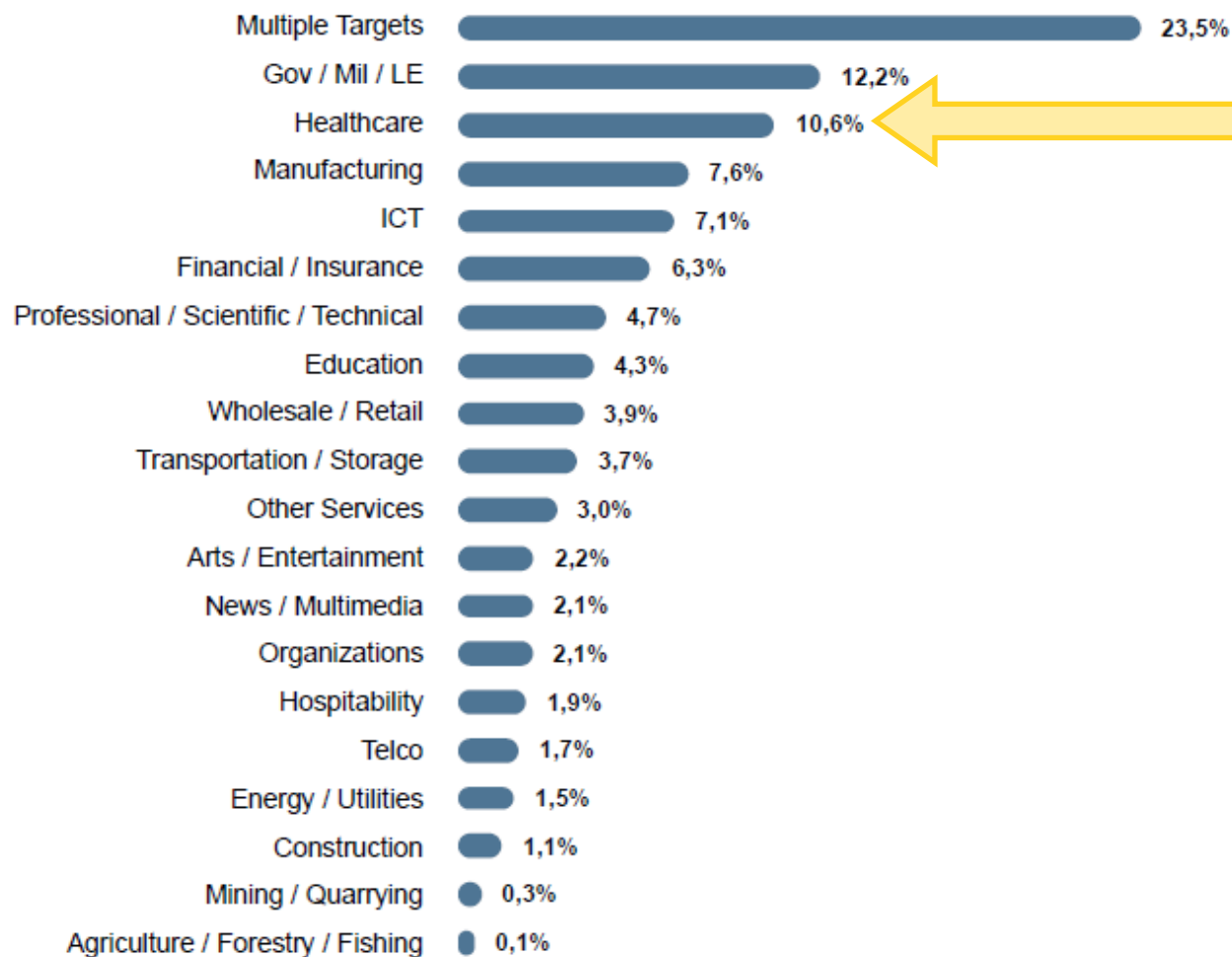
giuseppe.bungaro@adeodata.eu





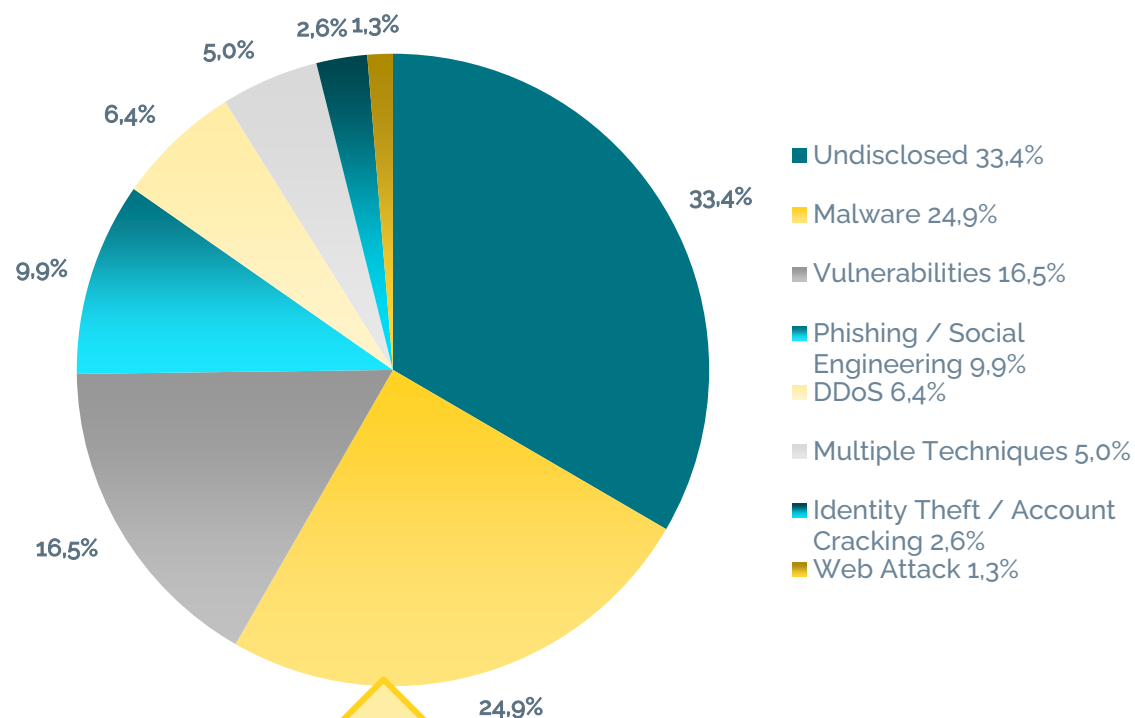
- Risultati Clusit 2026
- Evento avverso di Cybersecurity
- Classificazione degli incidenti NIS2 → GxP
- Pillole di NIS2
- NIS2-Annex 11-GAMP5-new Annex 11
- Legame tra GAMP5 e NIS2
- Il supporto di Adeodata per la Cybersecurity
- I servizi Digital di Adeodata

Distribuzione delle vittime 2025



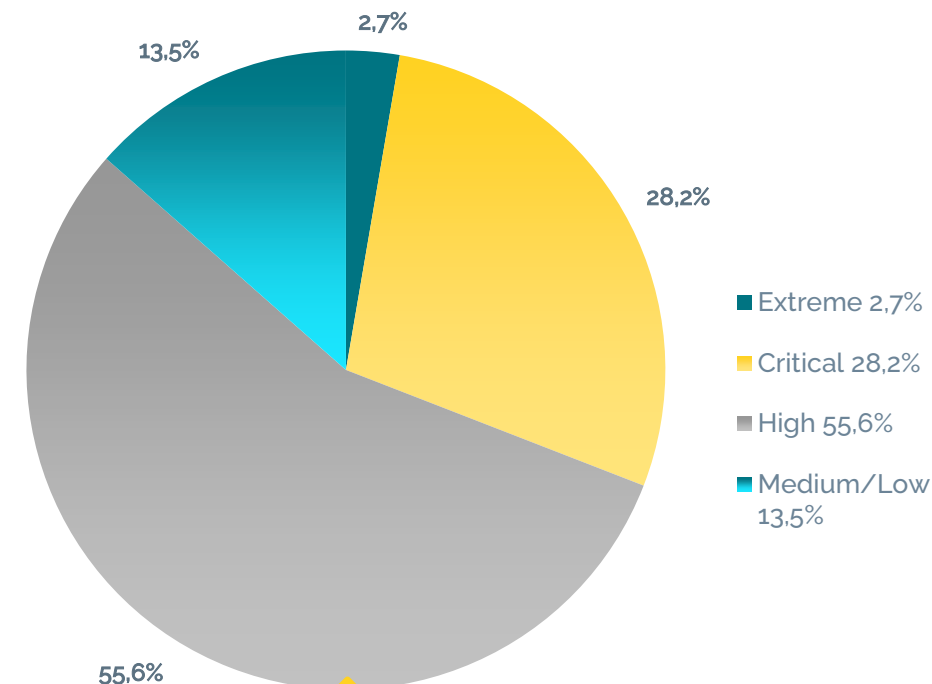
L'Healthcare è al terzo posto in termini di numerosità di attacchi

Distribuzione delle tecniche di attacco 2025



Malware e Vulnerabilità
sono le falle più sfruttate

Severità degli incidenti Cyber 2025



Quando avviene un evento
avverso Cyber è grave

1. Attacco

Un hacker sottrae le credenziali utente accedendo ai sistemi, anche quelli GxP critici.

2. Data Integrity

L'hacker rimane nella rete girando tra i sistemi e accedendo a dati sensibili.

3. Profili utente

...individua le credenziali degli utenti di alto livello

4. Gestione accessi

...ottiene le credenziali amministrative, che permettono l'accesso completo a tutti i sistemi.

5. Backup

Continua a girare nella rete, anche per mesi, fino ad individuare il modo per bloccare il sistema di backup.

6. Business Continuity

Solo a questo punto l'hacker fa partire la cifratura di tutti i sistemi, anche del sistema di backup.

Questo è lo scenario da chiarire quando si parla di sicurezza con il QA!



Fino a qualche tempo fa,
se un sistema GxP non era più disponibile, l'impatto era:

BASSO

per le GxP, perché non
alterava le funzionalità
convalidate*

ALTO

per NIS2, perché il sistema
non era solo bloccato, ma
perso

* Nella mera ipotesi che l'hacker avesse solo bloccato l'utilizzo del sistema e non alterato funzionalità e dati dello stesso → impatto su qualità del prodotto e Data Integrity

- Fino a pochi anni fa neanche l'IT prendeva in considerazione l'evento Cyber nella sua Risk Analysis.
- Il problema non esisteva e non era gestito.
- I dati ufficiali del Clusit 2026 ci dicono che un **evento Cyber non solo è molto probabile, ma se accade è anche distruttivo!**



**Possiamo, ancora oggi, non considerare
questo evento avverso?**

Gli incidenti con queste caratteristiche devo essere segnalati obbligatoriamente



IS-1

Il soggetto NIS ha evidenza della **perdita di riservatezza**, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale



IS-2

Il soggetto NIS ha evidenza della **perdita di integrità di dati** di sua proprietà o sui quali esercita il controllo, anche parziale.



IS-3

Il soggetto NIS ha evidenza della **violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività**.



IS-4

Il soggetto NIS ha evidenza dell'**accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà** o sui quali esercita il controllo, anche parziale.

In Italia, il recepimento è avvenuto
con il D.lgs. 138/2024



Concepita per contrastare l'aumento
delle minacce informatiche

Introduce stringenti requisiti di
Governance (ruoli, organizzazione e
procedure), gestione dei rischi e
segnalazione degli incidenti



Coinvolge i vertici aziendali

Prevede sanzioni



Il ruolo di Autorità Nazionale
competente è svolto dall'Agenzia
per la Cybersicurezza Nazionale
(ACN)

La NIS2 non è una
Linea Guida, è un
Decreto legge
→ **è quindi un
obbligo di legge!**

La NIS2 non è una
norma tecnica, ma
una norma di
Governance

È una normativa
**chiara, strutturata e
pratica**



Agenzia per la
cybersicurezza nazionale

Servizi essenziali

- Energia
- Trasporto
- Banche
- Infrastruttura del mercato finanziario
- **Sanità e servizi sanitari**
- Acqua potabile
- Acque reflue
- Infrastruttura di telecomunicazione
- Pubblica amministrazione
- Spazio

Servizi importanti

- Settore postale e spedizioni
- Gestione/Trattamento rifiuti
- **Settore chimico: produzione e distribuzione**
- **Settore alimentare: produzione, trasformazione e distribuzione alimenti, i.e. inclusa grande distribuzione**
- Industrie tecnologiche e ingegneristiche
- Servizi digitali
- Ricerca



FORNITORI E SERVICE PROVIDER DEI:

- Servizi essenziali
- Servizi importanti



Agenzia per la
cybersicurezza nazionale

Escluse, a meno
che non siano
ritenute di
importanza
critica

Grandi organizzazioni

> 250 dipendenti
> 50 M€ di fatturato

Medie organizzazioni

50 ÷ 250 dipendenti
> 10 M€ di fatturato

Piccole
organizzazioni

< 50 dipendenti
< 10 M€ di fatturato

Servizi essenziali

possono incorrere in multe fino a **10 milioni di euro o il 2%** del loro fatturato annuo globale.

Servizi importanti

possono incorrere in multe fino a **7 milioni di euro o l'1,4%** del loro fatturato annuo globale.

Le sanzioni **non riguardano** la valutazione delle **misure tecniche** di sicurezza implementate, ma **riguardano** la valutazione dell'**impianto di Governance**, processi, procedure messo in piedi dall'azienda.



Agenzia per la
cybersicurezza nazionale



Transposed (EU Member States):

Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden

Draft Law (EU Member States):

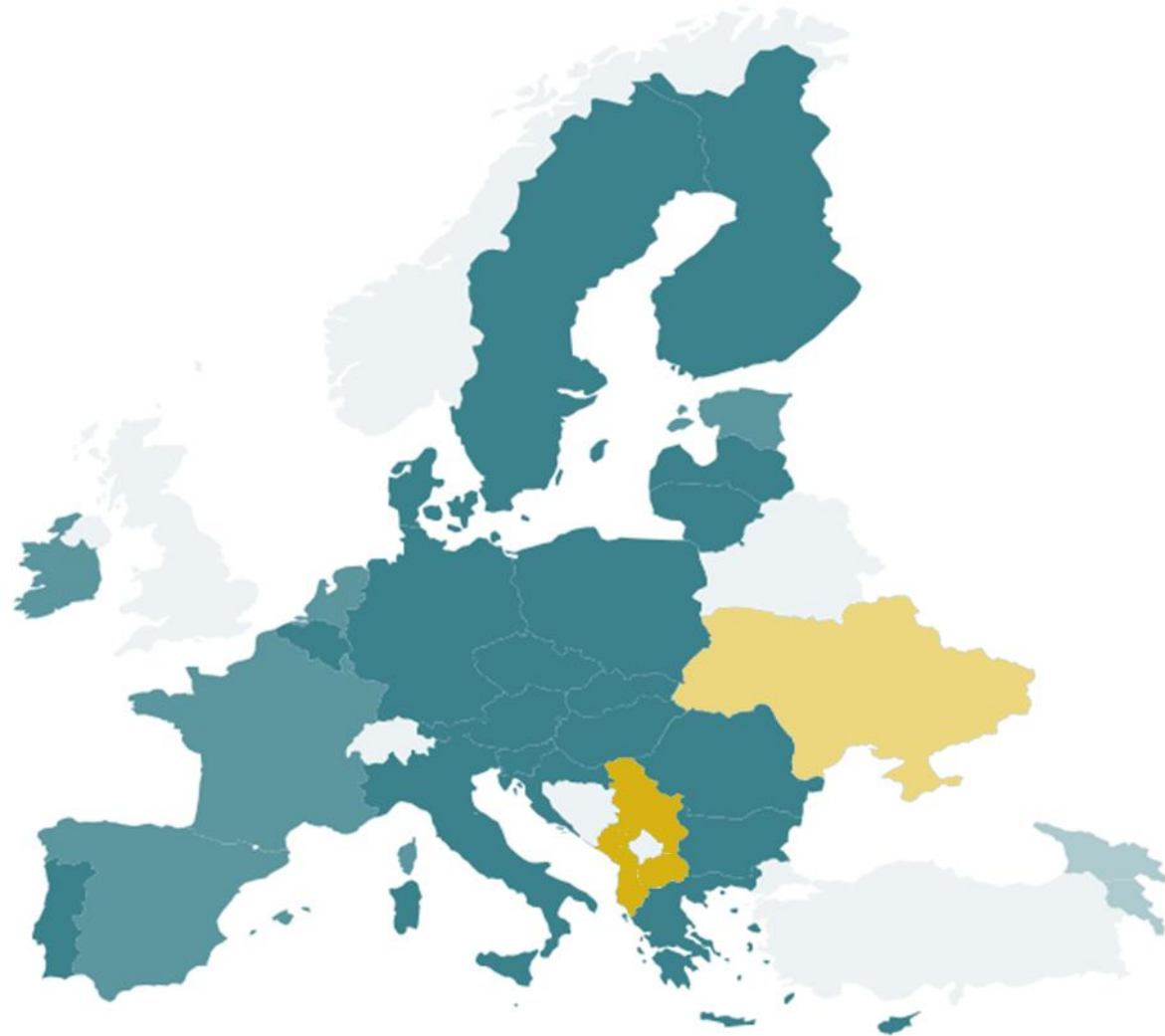
Estonia, France, Ireland, Netherlands, Spain

Transposed (Non-EU Member States):

Albania, Montenegro, North Macedonia, Serbia

Draft Law (Non-EU Member States):

Armenia, Georgia, Moldova, Ukraine



Fonte: ecs-org.eu – aggiornamento 6 marzo 2026

Art. 23

Organi di amministrazione e direttivi

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;

b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7;

c) sono responsabili delle violazioni di cui al presente decreto.

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) sono tenuti a seguire una formazione in materia di sicurezza informatica;

b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

3. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.



2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

- a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;
- c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
- d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

- e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
- f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- g) pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
- i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
- l) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.



- 9 Appendix M1 - Validation Planning
- 10 Appendix M2 - Supplier Assessment
- 11 Appendix M3 - Science-Based Quality Risk Management
- 12 Appendix M4 - Categories of Software and Hardware
- 13 Appendix M5 - Design Review and Traceability
- 14 Appendix M6 - Supplier Quality Planning
- 15 Appendix M7 - Validation Reporting
- 16 Appendix M8 - Project Change and Configuration Management
- 17 Appendix M9 - Documentation and Information Management
- 18 Appendix M10 - System Retirement
- 19 Appendix M11 - IT Infrastructure
- 20 Appendix M12 - Critical Thinking



21 Appendix D1 - Specifying Requirements

22 Appendix D2 - (Retired)

23 Appendix D3 - Configuration and Design

24 Appendix D4 - Management, Development, and Review of Software

25 Appendix D5 - Testing of Computerized Systems

26 Appendix D6 - System Descriptions

27 Appendix D7 - Data Migration

28 Appendix D8 - Agile Software Development

29 Appendix D9 - Software Tools



32 Appendix 0 - Introduction to Operation Appendices

33 Appendix 01 - Handover

34 Appendix 02 - Establishing and Managing Support Services

35 Appendix 03 - System Monitoring

36 Appendix 04 - Incident Management and Problem Management

37 Appendix 05 - Corrective and Preventive Action

38 Appendix 06 - Operational Change and Configuration Management

39 Appendix 07 - (Retired)

40 Appendix 08 - Periodic Review

41 Appendix 09 - Backup and Restore

42 Appendix 010 - Business Continuity Management

43 Appendix 011 - Security Management

44 Appendix 012 - System Administration

45 Appendix 013 - Archiving and Retrieval





46 Appendix S1 - Alignment with ASTM E2500.

47 Appendix S2 - Electronic Production Records

48 Appendix S3 - End User Applications Including Spreadsheets

49 Appendix S4 - Patch and Update Management

50 Appendix S5 - (Retired)

51 Appendix S6 - Organizational Change

- Sicurezza
- CMDB
- Test
- Gestione degli Incidenti
- Patch vulnerabilità
- Upgrade
- Governance dell'infrastruttura
- ITIL
- Incident
- Problem
- Change
- Accessi
- Business Continuity
- Backup e Restore



EUROPEAN MEDICINES AGENCY
 SCIENCE MEDICINES HEALTH

9 March 2023
 EMA/INS/GCP/112288/2023
 Good Clinical Practice Inspectors Working Group (GCP IWG)

Annex 4 Security	36
A4.1 Ongoing security measures	36
A4.2 Physical security	36
A4.3 Firewalls	36
A4.4 Vulnerability management	36
A4.5 Platform management	37
A4.6 Bi-directional devices	37
A4.7 Anti-virus software	37
A4.8 Penetration testing	37
A4.9 Intrusion detection and prevention	37
A4.10 Internal activity monitoring	37
A4.11 Security incident management	38
A4.12 Authentication method	38
A4.13 Remote authentication	38
A4.14 Password managers	38
A4.15 Password policies	39
A4.16 Password confidentiality	39
A4.17 Inactivity logout	39
A4.18 Remote connection	39
A4.19 Protection against unauthorised back-end changes	39



NIS2 Governance

Governance della Cybersecurity

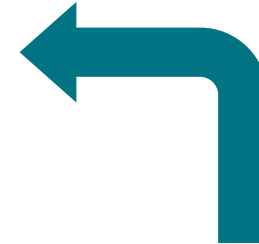
Responsabilità del CdA
Ruoli e responsabilità
Deleghe
Risk Analysis
GAP Analysis
Gestione degli Incidenti
Gestione della crisi

GAMP



Business Continuity e Disaster Recovery
Backup & Restore
Gestione della patch e vulnerabilità
Gestione degli asset informatici, CMDB
Classificazione e integrità dei dati

Miglioramento continuo
Review periodiche
Fornitori qualificati/rilevanti
Formazione periodica
Audit interni



NIS2 Attività Tecniche

MFA
Crittografia
Gestione accessi
Gestione firewall
Segmentazione rete

Il **QA** lavora per la compliance GxP



La **Sicurezza** lavora per elevare i livelli di security

L'**IT** lavora per gestire la rete e i dati



L'**OT** lavora su tutte queste cose ma in maniera autonoma



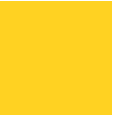
Per l'IT

Supportiamo il reparto IT ad implementare la Governance della Cybersecurity (coinvolgendo il QA).



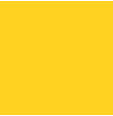
Per l'OT

Supportiamo il reparto OT a comprendere la Governance della Cybersecurity e a integrare i requisiti NIS2 e GxP.



Per il QA

Supportiamo il reparto QA a comprendere la Governance della Cybersecurity e a integrare i requisiti GxP.



Maintenance

- Review periodiche
- Miglioramento continuo



Convalide

Valutiamo e armonizziamo i principi di
convalida GxP con i requisiti NIS2

Adeodata ha competenza ed esperienza su:

- Cybersecurity Governance NIS2
- Infrastrutture e sistemi GxP

Grazie al supporto di Adeodata:

- La Governance di Cybersecurity NIS2 viene definita tenendo in considerazione aspetti e requisiti GxP.
- Procedure e flussi di Cybersecurity vengono integrati nei protocolli di convalida.



ADEODATA

LIFE. SCIENCE. SERVICE.







Bregnano (Como)



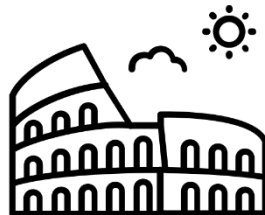
Parma



Padova



Lugano 
Svizzera



Roma



Ancona

PMO per progetti di
digitalizzazione



Business Intelligence

Digital Process Design



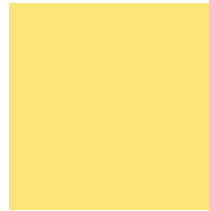
Software Selection

Governance di Cybersecurity



Compliance GxP & NIS2

Digital Transformation con
SAP: analisi processi GxP e
integrazione nei flussi QA

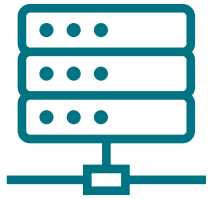


Analisi processi reparto R&D,
spunti di efficientamento e
Software Selection

Project Management per
implementazione sistema
gestione Batch Record



Servizi AI, Audit e Governance

**30**

Validated ERP
(2022-2024)

**>1.400**

Service days for IT
systems that
monitor/manage the
equipment of 2 new
sterilization departments
(2024-2025)

**>1.000**

Service days for IT
systems updated
following the installation
of new infrastructure
(2024-2025)

**>70**

Data Integrity
assessments
(since 2015)



EMAIL

giuseppe.bungaro@adeodata.eu



TELEFONO

+39 340 8004700



SITI WEB

www.adeodata.eu

www.qualitysystems.it

GRAZIE!