Gamp5 (2nd Edition) e la Security

Enzo M Tieghi – etieghi@servitecno.it

ServiTecno

INDICE

Introduzione

Le “nuove” GAMP (Good Automated Manufacturing Practices), il “vangelo” per chi sviluppa e convalida sistemi computerizzati destinati all’utilizzo nell’industria del Life-Science (Farmaceutico, Biotech, Medical Devices, Nutritionals, ecc.) sono state pubblicate nel 2022 (l’edizione precedente era del 2005) ed il volume di oltre 400 pagine tra testo, appendici e glossari ha come sottotitolo “A Risk-Based Approach to Compliant GxP Computerized Systems”.

Come enunciato nell’incipit, la Guida, creata dal gruppo di lavoro Gamp di ISPE (**www.ispe.org**, l’associazione internazionale che raggruppa i professionisti dell’industria Life Science), ha lo scopo di essere di supporto alle aziende dei comparti regolati dalle GxP (le linee guida per lo sviluppo, produzione e distribuzione di farmaci): non è un documento di regolamentazione, non è uno standard “de Jure” e non è automatico che sistemi sviluppati in accordo alle Gamp vengano accettati dalle autorità di vigilanza e controllo in ambito farmaceutico, che operano secondo protocolli condivisi a livello sovranazionale. Ricordiamo che per le regolamentazioni bisogna fare riferimento in Italia all’Agenzia Italiana del Farmaco, mentre l’organo di supervisione dell’Unione Europea è la European Medicines Agency (EMA). Negli Stati Uniti e per tutti gli stabilimenti che intendono esportare prodotti negli USA opera invece la U.S. Food and Drug Administration (FDA).

È però innegabile che le GAMP siano uno standard industriale “de Facto” alle quali si attengono tutti i partecipanti alla catena di fornitura nell’industria farmaceutica, dai costruttori di macchinari ed impianti, ai produttori e fornitori di materie prime, semilavorati, principi attivi, prodotti complementari e di confezionamento, consulenti e fornitori di servizi per l’industria del Life Science e naturalmente tutti i produttori e confezionatori di farmaci operanti nei paesi soggetti a stringenti regolamentazioni del settore.

Nella prefazione di questa seconda edizione della GAMP5, che volutamente non sono passate alla numerazione GAMP6 proprio per dare continuità di visione, si fa presente che il recente periodo di pandemia globale di Codid-19 ha sottolineato il ruolo essenziale delle nuove tecnologie per la protezione della salute pubblica: in particolare questa guida GAMP5 tende a promuoverne l’utilizzo proprio per salvaguardare la qualità del prodotto e la sicurezza per il paziente.

Le innovazioni sono essenziali per l'Industria del Life Science per aumentare il valore per l'intera società, controllando i costi e ridurre il time-to-market.

La vasta regolamentazione di questo settore industriale potrebbe portare ad adottare approcci troppo rigidi per rispettare le norme, che spesso non sono commisurati all'effettivo rischio in essere per la qualità del prodotto e la salute per il paziente: in questa visione la revisione delle GAMP5 propone innovazione per la valutazione del rischio ed un uso efficiente ed efficace delle risorse anche applicando nuovi approcci nello sviluppo di sistemi ed utilizzo di tecnologie di mercato.

La Security nelle GAMP5

Già nell'edizione precedente delle GAMP5 era presente la appendice "**O11 – Security Management**", che però per la consapevolezza sul tema di quando era stata scritta, era abbastanza stringata e poco utile per chi doveva occuparsi della protezione dal rischio cyber di reti e sistemi di fabbrica, macchinari ed impianti utilizzati nella produzione di farmaci.

Nell'introduzione della "nuova" appendice O11 si descrive la Gestione della Security come le "considerazioni organizzative, di processo e tecniche che possano assicurare riservatezza, integrità e disponibilità dei sistemi computerizzati, dati e records in un'azienda attiva in ambito regolato", sottolineando come un'efficace gestione delle security minimizzi il rischio di minacce dall'interno e dall'esterno. Tra in veri aspetti di cambiamento rispetto alla versione precedente delle GAMP, vediamo che ora richiede un allineamento ai sistemi di gestione ed alle pratiche di IT Security descritte sia nelle ISO27001 che nei framework di NIST.

Rammentiamo che la ISO27001, nella sua versione più recente ovvero quella del 2022, è incentrata principalmente sulla "Sicurezza delle Informazioni" in tutte le forme e supporti (cartacei, cloud, digitali e verbali)", la cybersecurity e la protezione dei dati personali attraverso l'istituzione all'interno delle organizzazioni di un sistema di gestione relativo proprio alla sicurezza delle informazioni.

Dalla prima versione del 2005 della ISO/IEC 27001 (e prima ancora dalla BS7799 del 1997), molte cose sono cambiate nel modo di proteggere i sistemi informativi e quanto questi supportano, a partire dallo stesso nome che, da sicurezza "informatica", o addirittura "logica", è passato a sicurezza delle "informazioni" per poi essere comunemente ed impropriamente scambiato per CyberSecurity.

La ISO/IEC 27001 è poi ulteriormente cambiata nel 2013, principalmente legata all'introduzione della "high-level structure", oggi comune a tutti i sistemi di gestione riferiti ad ISO. Ora con questa nuova versione del 2022 vediamo evidenziati parte dei controlli presenti nella sua appendice A, e che poi saranno ulteriormente puntualizzati anche nella conseguente ISO27002, anch'essa pubblicata nella seconda parte del 2022.

Notiamo che queste Gamp5 sono state pubblicate prima della ISO27001:2022, dobbiamo allora valutare se questa appendice O11 delle GAMP5 seconda edizione, sia più "aderente" alla ISO27001:2013 o alla ISO27001:2022, visto che nelle note di riferimento si menziona solo la prima.

Dobbiamo anche verificare se il riferimento al NIST, citato all'inizio, sia più congruo riportarlo al NIST CyberSecurity Framework in vigore al momento della pubblicazione, ovvero quello ancora presente sul sito di NIST nel 2022. Segnaliamo infatti che è in corso proprio una revisione per aggiornare il CyberSecurity Framework di NIST alle nuove metodologie di sviluppo e tecnologie oggi disponibili sul mercato, revisione attesa in questo 2023.

Da sempre la "Security Management" prende come criteri di protezione quelli derivati dalla triade C-I-A, ovvero Riservatezza, Integrità, Disponibilità delle Informazioni. Sin dalla sua prima edizione lo standard IEC62443 ha definito le priorità per la OT Security esattamente all'inverso, ovvero A-I-C, mettendo come primo requisito quello della Disponibilità dell'informazione, per poi avere Integrità e per ultimo in termini di priorità quello della Riservatezza. Ricordiamo che IEC62443 è ripresa proprio dallo standard NIST-SP800-83, poi identificato dal NIST Cyber Security Framework come lo standard da utilizzare per la security dei sistemi di controllo ed automazione nell'Industria, anche quella farmaceutica.

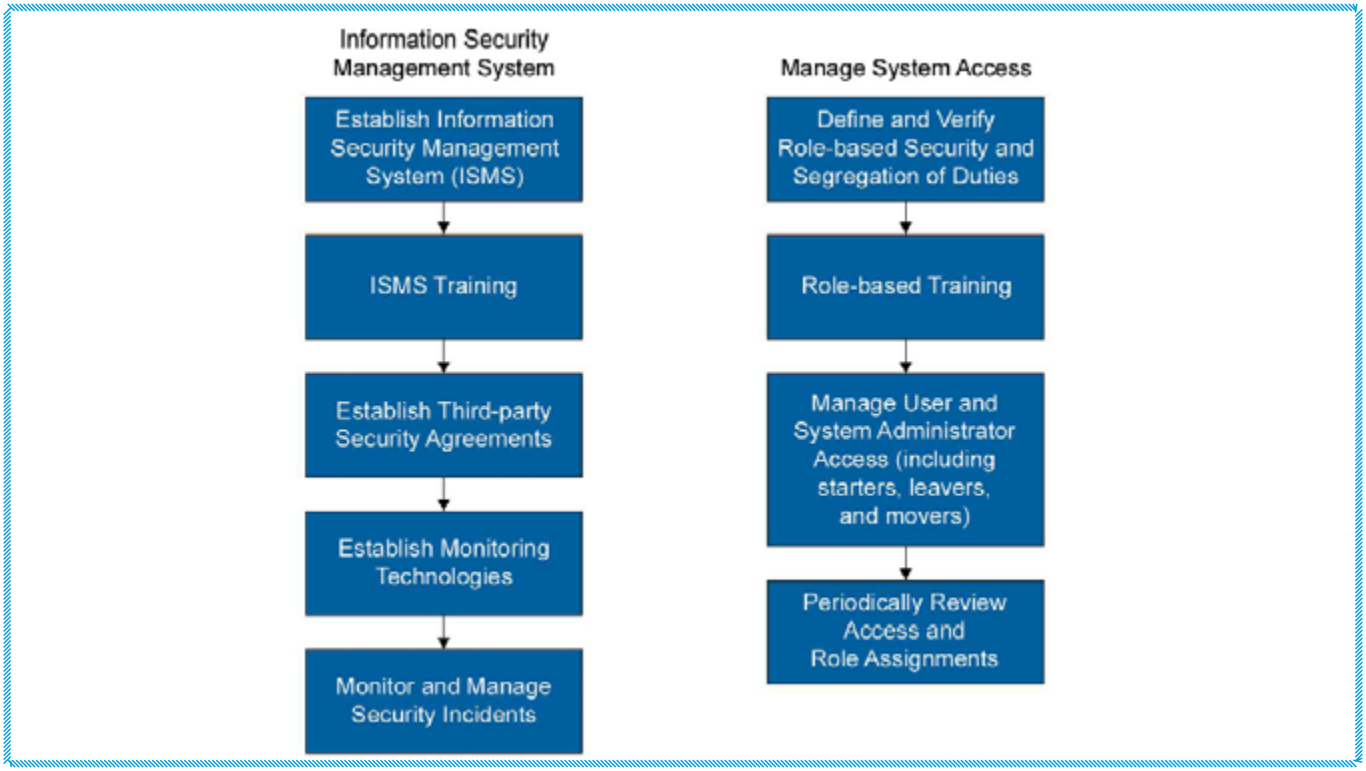
Vorremmo qui anche sottolineare che il requisito della "Integrità" è il mantra ormai utilizzato da anni in tutte le regolamentazioni riferite alla "Data Integrity" nel mondo del Life Science, con alcuni documenti emessi da FDA e da EMA, rimanda proprio specificamente ad aspetti da preservare e conosciuti come ALCOA ed ALCOA+. Ma questo è un altro tema da approfondire a latere (vedi appendice sulla Data Integrity, in coda).

Requisiti Chiave per la gestione della Security.

Si richiedono le seguenti misure di sicurezza:

- Impostare e mantenere controlli organizzativi, procedurali e tecnici per minimizzare il rischio di accessi non autorizzati a sistemi, dati, records
- Avere un sistema di accessi role-based per utenti ed amministratori, con attenzione alla separazione di ruoli e compiti
- Implementare un monitoraggio manuale ed automatizzato dei sistemi computerizzati e degli ambienti per identificare ed eventualmente rispondere a potenziali vulnerabilità ed intrusioni
- Avere in mente i processi di gestione degli incidenti e dei problemi per valutare e mitigare i potenziali rischi per la sicurezza
- I controlli di sicurezza dovrebbero essere continuamente valutati per affrontare e rispondere alle nuove minacce per l'ambiente informatico.
- L'ambito delle misure di sicurezza dipende da diversi fattori, tra cui l'ambito e la criticità dei processi regolamentati, dei record e dei dati conservati dal sistema e se il sistema computerizzato è interfacciato con l'esterno (ovvero, connesso a Internet).

La figura qui sotto, riporta il flow dei processi coinvolti nella implementazione di un sistema di gestione della security, in relazione alla elevazione del Livello di Maturità. (N.B. la figura qui riportata è tratta dalle GAMP5/2022, appendix O11)



Controlli organizzativi per la gestione della Security

Le misure organizzative richiedono che il personale addetto al sistema, inclusi fornitori e consulenti, abbia chiare le responsabilità e doveri rispetto a funzioni, processi e ai dati soggetti a regolamentazione.

Devono essere intraprese periodiche attività di training e sensibilizzazione per fare in modo che il personale capisca i rischi relativi alla sicurezza delle informazioni.

Ruoli e responsabilità devono essere chiaramente definiti e comunicati a tutta l'organizzazione.

Prima dell'assunzione di personale nuovo è necessario valutare se i candidati siano adeguati alla posizione per evitare potenziali rischi dovuti a comportamenti illeciti.

Il sistema di gestione per la sicurezza delle informazioni (ISMS)

Bisogna prevedere un ISMS (come quello definito nella ISO2700x) che definisca politiche, procedure e strumenti da adottare per proteggere dati e sistemi computerizzati. I riferimenti che troviamo a fianco di alcune delle voci indicate, sono riferite a capitoli ed appendici delle GAMP5 stesse, ove vengono trattati specificamente e qui richiamati:

- Sicurezza delle informazioni
- Gestione delle risorse umane
- Gestione del rischio (capitolo 5)
- Classificazione e gestione delle informazioni
- Identificare e gestire chi può accedere al sistema (con revisione periodica)
- Separazione dei compiti/ ruoli
- Gestione dei cambiamenti (appendice O6)
- Gestione incidenti (appendice O4)Protezione antimalware
- Gestione record e documenti (appendice M9)
- Qualifica e Gestione fornitori (appendice M2)
- Backup & Restore (app. O9)
- Archiviazione e Manutenzione dati nel tempo (app. O13)

- Business Continuity e Disaster Recovery (app. O10)
- Gestione della sicurezza della rete
- Gestione patch
- Gestione Vulnerabilità
- Gestione dispositivi mobile e telelavoro
- Controllo e sincronizzazione dei clock di sistema
- Sviluppo e manutenzione software applicativo (appendici D)
- Gestione degli asset informatici
- Classificazione dei dati
- Gestione e smaltimenti dei supporti/media
- Condivisione e trasferimento delle informazioni
- Adeguamenti alle regolamentazioni locali sulla privacy
- Audit interni del ISMS

Si può notare che molti dei requisiti possono essere già insiti nei sistemi di qualità per la compliance GxP, in particolare quelli dei sistemi di Qualità IT: in ottica di semplificazione è auspicabile una aggregazione e integrazione tra i diversi framework a livello di politiche e procedure.

Controlli Fisici e Tecnologici

Controlli fisici e tecnologici dovrebbero essere implementarti per minimizzare il rischio di accessi non autorizzati o involontari ai sistemi computerizzati. Ecco alcuni esempi di questi controlli:

- Security in base a ruolo
- Accesso in base a ruolo
- Gestione accessi ed identità (con autenticazione multi-fattori MFA)
- Controlli per la gestione password
- Segmentazione degli ambienti
- Crittografia dei backup
- Restrizioni sui software installabili
- Software anti-phishing
- Sicurezza Rete
- Implementazione e gestione VPN
- Crittografia dei Dati (sia dati residenti che in transito, valutando i rischi)
- Gestione delle chiavi (crittografiche)
- Scansione (periodica) vulnerabilità
- IDS/IPS (Intrusion Detectio/Prevention)
- PT (penetration test)
- Firewall e controllo/prevenzione perimetrale
- Protezione dispositivi endpoint

- Controlli per l'accesso fisico ai reparti/uffici/laboratori, includendo sala server e data center, armadi dei server, ecc.
- Segmentazione logica
- Controllo/gestione reti "guest" e Wi-Fi
- Politiche di "clear screen" e "clear desk"

Monitoraggio e Gestione incidenti

È richiesto di monitorare le minacce, soprattutto quando i sistemi computerizzati hanno connessioni con l'esterno. Da valutare se con tool di monitoraggio automatizzati e/o con strumenti manuali per:

- Identificare intrusioni
- Identificare Vulnerabilità
- Identificare rotture SW e HW
- Identificare variazioni nelle configurazioni non autorizzate
- Monitorare l'utilizzo delle risorse
- Identificare interruzioni sulla rete
- Controllo periodico degli accessi

Quando possibile, i tool per il monitoraggio dovrebbero automaticamente informare chi si occupa della security per aprire ticket che possano portare alla investigazione e mitigazione dei potenziali rischi cyber.

Ambienti CLOUD

Gli ambienti Cloud sono costantemente a rischio di minacce cyber sofisticate che potrebbero portare a infrazioni e sottrazioni di dati, nonché ad interruzioni di servizio. Un robusta Cloud security, è una responsabilità condivisa tra chi fornisce infrastruttura, la piattaforma ed le applicazioni (IaS, Pas, AaS).

Ne conseguono le seguenti considerazioni da valutare:

- Risorse umane
- Geolocalizzazione e protezione dati
- Sicurezza applicativa
- Monitoraggio delle configurazioni (attenzione alle variazioni nelle configurazioni ed infrastrutture)
- Sicurezza dei sistemi operativi
- Reti fisiche e virtuali
- Server e storage
- Monitoraggio dei servizi e fornitori di Cloud

Le architetture Cloud devono avere adeguate segregazioni fisiche e logiche dei server, dei servizi, e dei dati per minimizzare rischi di security che possano avete impatti sull'ambiente Cloud intero e su altri utenti connessi.

Una gestione centralizzata delle policy di security assicura una efficace applicazione dei controlli aggiornati su tutto l'ambiente Cloud.

Come sappiamo le API (application program interface) gestiscono gli accessi ai dati, alle applicazioni ed ai servizi: ne consegue che il disegno e sviluppo delle API deve includere una robusta security per minimizzare il rischio di accessi non autorizzati.

È anche auspicabile adottare contromisure nei confronti di possibili DOS (Denial of Service).

Aziende soggette a regolamentazione devono utilizzare solo fornitori di Cloud che possano garantire appropriati livelli di servizio e di sicurezza.

Un esempio di Cloud Security condiviso a livello internazionale può venire dal **CSA STAR**: uno schema di certificazione della sicurezza dei servizi cloud che consente alle aziende di ottenere una certificazione internazionale sull'affidabilità, sicurezza e trasparenza dei servizi cloud offerti.

Lo schema di certificazione CSA STAR si integra nel sistema di gestione **ISO27001** attraverso l'utilizzo della **Cloud Control Matrix** **(CCM)** con cui vengono aggiunti dei controlli specifici sulla sicurezza cloud (**197** controlli suddivisi in **17** Domini). Lo schema di certificazione CSA STAR è conforme alle norme ISO17021, ISO27006, ISO19011. CSA STAR è il primo e ad oggi, nel 2023, ancora unico schema di certificazione universalmente condiviso che misura la «**maturità**» dei controlli di sicurezza implementati (livelli: Bronze, Silver, Gold). Attualmente si contano **+2000 aziende certificate nel mondo** (tra cui Google, AWS, Microsoft, IBM, ...) di cui **+300 in Italia**. (N.B. controllare quale configurazione di CLOUD risulta certificata CSA STAR)
Il programma CSA STAR è oggi proposto in due livelli:

- **Livello #1** (Autovalutazione): è sufficiente compilare il questionario **CAIQ** e pubblicarlo nello STAR Registry di CSA
- **Livello #2** (Audit di Terza Parte): effettuato da una società di certificazione di sistema **qualificata CSA STAR Auditor**

Per maggiori informazioni.

I Cloud Service Provider propongono di solito diversi tipi di SLA (Service Level Agreement): il livello di SLA consigliato deve includere la security con servizi di monitoraggio inclusi.

Piani di DR Disaster Recovery (come indicato nell'appendice GAMP O10) devono prevedere che le responsabilità per i Cloud provider di infrastruttura, piattaforma ed applicativi siano chiaramente definite e coordinate in caso di incidente di rilievo e per tutta la durata dell'interruzione fino al ristabilimento di condizioni di funzionamento.

Naturalmente è necessario che siano presenti e testati i piani per backup e ripartenze e di tutti i componenti della DR.

AUDIT

Si devono prevedere programmi di audit, basati sul rischio, con assesment sui controlli organizzativi, fisici, tecnologici e dei processi

Management Review

Il Senior Management dovrebbe periodicamente verificare l'efficacia dei controlli di sicurezza, assicurando che ci siano adeguati budget di investimenti e risorse che possano garantire la protezione dei dati GxP.

Patch di sicurezza e compliance GxP

Le patch di sicurezza (come indicato nell'appendice GAMP5 S4) e gli aggiornamenti dei sistemi operativi e degli applicativi vengono rilasciati dai fornitori su base regolare: di solito queste patch risolvono vulnerabilità e difetti con impatto sulla security.

Il rischio che queste patch abbiamo impatti sulla corretta funzionalità dei sistemi è di solito basso e quindi anche l'impatto sullo stato di convalida di tali sistemi computerizzati si suppone sia basso. Si possono quindi adottare approcci per valutare il rischio connesso all'aggiornamento prima di entrare in produzione e quindi procedere con:

- Risk assessment per il rilascio delle patch
- Rilascio delle patch per testare/validare l'ambiente di test prima di andare in produzione
- Rilascio delle patch su ambienti non GxP rilevanti, prima di essere rilasciate su ambienti GxP

Programmi di Certificazioni di Security

In questa appendice O11 delle GAMP5 2nd Rev. vengono menzionati alcuni schemi di certificazione di sicurezza di terze parti da utilizzare come riferimenti ai sistemi di gestione della sicurezza delle informazioni nei Service Provider da valutare come fornitori: ISO270017, ISO2700x, AICPA SOC1,2,3.

Si prega quindi di porre attenzione a valutare la validità e l'estensione di queste certificazioni e soprattutto verificare il perimetro al quale queste certificazioni sono attribuite.

Matrice di riferimento Security nelle GAMP5 Second Edition

(legenda: in questa matrice vengono riportati i punti presenti nelle GAMP5 ove si menziona un riferimento al termine “security”, sia con riferimento alla security “logica” che a quella “fisica”)

Main Body / Appendix	Pagina	Ref.
2.2	22	The system owner is responsible …
3.1	24	Maintaining control (including security….)
Table 4.2	42	Security and System Administration
4.3.7	46	Security Management
6.1.1	56	Security Management
6.2.3.1	61	Process Owner coordinating …
6.2.3.2	61	The system owner is responsible …
6.2.5.3	65	Supplier Assessment and Education
7.13	76	System Support and Maintenance During Operation
8.5.3	81	Secondary Test evidence
M2 10.4.3.3	99	Audit
M2 10.10	106	International Standards and Certification
M3 11.5.3.3	115	Functional Risk Assessment
M3 11.5.3.5	116	Risk Based Decisions during Planning
M4 12.3.1	129	Category 1 - Infrastructure Software
M10 18.3.2.8	161	System Maintenance
M11 19.1	163	IR Infrastructure
M11 19.2.4	165	Infrastructure Automation
M11 19.3	165	Risk Management Infrastructure
M11 19.5.1	167	Security Management
M12 20.3.8.1/2	178	Critical Thinking
D1 21.3.1	184	Specifing Requirements
D1 21.3.3.3	188	Security includinf Access Control
	189	Data Security and Integrity including access
	190	Interfaces / Access and Security
	191	Environment / Physical security
D3 23.3.3.	201	Configuration
	203	Encryption

Main Body / Appendix	Pagina	Ref.
	204	Cloud + Multitenent
D4 24.3.3.2	211	Software / Free + Open Source
D5	231	Testing / Security Procedures
	232	Points to consider for all systems
D6	235	Intro / ex Annex 11
D6 26.3.2.4	236	Firewall
D6 26.3.2.8	237	Security Controls
D8 28.3.5	250	Agile Software Dev Approvals
D8 28.3.6	250	DevOps vs. Security
D8 28.4	251	Agile Approach to Quality
D9 29.2	254	Software Tools / Scope
D9 29.3.2	254	Risk Assesment
D9 29.3.6 / 7	255	Security Considerations - Data and Records
D10 + D11	258 /269	Block Chain / AI / ML
O2	289	Establishing and Maintaining Support Services
O3	291	System Monitoring
O5	301	CAPA Process
O6	307	Change Management
O8	314	Periodic Review
O9	323	Backup and Restore
O10	327	Business Continuity Management
O11	331	Security Management
O12	337	System Administration
O13	345	Archiving and Retrieval
S2	351	Electronic Production Records
S3	361	End User Applications including Spreadsheets
S4	371	Patch and Update Management
S6	378	Organizational Change
G1	383	References
G2	399	Glossary

Appendice: Data integrity e non conformità nel farmaceutico

La non conformità dei processi può avere un impatto importante sulla produzione. Per questo è importante assicurare la integrale data integrity nel farmaceutico. Scopriamo come.

Per affrontare un tema complesso come quello della Data integrity nel settore farmaceutico, partiamo dalle definizioni. Secondo il Manuale della Qualità dell'Agenzia Italiana del Farmaco (AIFA), una non conformità è il mancato soddisfacimento di un requisito o una deviazione rispetto alle specifiche di riferimento. Le non conformità - che possono riferirsi al prodotto, al sistema, a un processo o a una procedura - vengono solitamente rilevate dai valutatori nel corso delle visite ispettive.

La conformità dei processi può essere garantita solo ed esclusivamente dai dati. In questa prospettiva, la data integrity assume un ruolo strategico per assicurare trasparenza e coerenza con le regolamentazioni nazionali e internazionali.

Data integrity nel farmaceutico: il contesto normativo

Ogni Paese dispone di un'autorità di vigilanza e controllo in ambito farmaceutico, che opera secondo protocolli condivisi a livello sovranazionale. In Italia esiste la già citata Agenzia Italiana del Farmaco, mentre l'organo di supervisione dell'Unione Europea è la European Medicines Agency (EMA). Negli Stati Uniti opera invece la U.S. Food and Drug Administration (FDA).

La data integrity nel farmaceutico presuppone regole e prassi comuni.

La Food and Drug Administration ha indicato cinque princìpi di conformità dei dati in ambito farmaceutico sintetizzati nell'acronimo ALCOA. I dati devono sempre essere:

- Attribuibili alla persona o attività che ha generato il dato
- Leggibili e permanenti
- Contemporanei e contestuali al processo da cui hanno avuto origine
- Originali
- Accurati

A questi principi si aggiungono quattro requisiti individuati dall'EMA e riassunti nell'acronimo CCEA:

- Complete: i dati devono essere raccolti dallo stesso campione
- Consistent: i dati devono essere raccolti in modo sequenziale attraverso un timestamp
- Enduring: i dati devono essere consistenti e conservati su un media resistente
- Available: i dati devono essere accessibili per consultazione durante tutto il loro ciclo di vita

Data integrity e non conformità

La non conformità dei dati può assumere sfumature diverse. Gli esempi in questa direzione sono molteplici. Per esempio, i dati possono non essere contestuali, possono cioè essere stati registrati in un momento diverso rispetto a quello indicato. I test possono poi essere stati eseguiti più volte per ottenere e registrare solo i risultati migliori. I dati possono inoltre essere stati manipolati in modi diversi, anche involontariamente.

In un contesto di massima sicurezza e rigide regolamentazioni come quello farmaceutico, la non conformità può avere conseguenze importanti per le aziende produttrici e avere impatti profondi sul posizionamento di mercato.

In questa prospettiva, la FDA ha individuato sei domande principali a cui rispondere per garantire la data integrity nel farmaceutico:

1. Al momento dell'esecuzione, tutte le attività sono state documentate?
2. Le singole attività possono essere attribuite all'operatore che le ha eseguite?
3. I registri di produzione possono essere modificati esclusivamente da personale autorizzato?
4. Esiste un registro relativo alla variazione dei dati?
5. I registri sono stati analizzati per assicurare accuratezza, completezza e conformità agli standard?
6. I dati vengono mantenuti in modo sicuro dopo la loro creazione?

Come evitare episodi di non conformità

Evitare episodi di non conformità è possibile? La risposta è sì. Vediamo come. L'integrità dei dati, la coerenza dei processi di raccolta e la massima trasparenza in ottica ispettiva possono essere raggiunti attraverso l'implementazione di piattaforme software di controllo e supervisione.

I sistemi SCADA accompagnati da un Historian sono quindi una risposta efficace e rappresentano uno strumento strategico in ottica di data integrity nei reparti di produzione per il settore farmaceutico.

Le soluzioni disponibili oggi sul mercato si caratterizzano per flessibilità e modularità, adattandosi alle diverse esigenze di produzione ma sempre nell'ottica del controllo completo del ciclo di vita del dato. Il tutto in modalità paperless e con la possibilità di interpretazione dei dati multi-piattaforma.

A partire dai princìpi e requisiti ALCOA-CCEA citati in precedenza, i sistemi SCADA+Historian permettono di rispettare le normative di conformità.

All'interno di una soluzione SCADA+Historian, infatti, i dati possono essere:

- Attribuibili alla persona, alla macchina all'impianto o alla attività che li ha generati
- Consultabili in tempo reale
- Generati e registrati in tempo reale attraverso timestamp
- Accurati, dal momento che non possono essere manipolati volontariamente o involontariamente dall'attività umana in quanto generati e registrati sulla macchina
- Raccolti sullo stesso campione e quindi completi
- Consistenti, in quanto registrati in modo automatico e sequenziale
- Resistenti nel tempo con la possibilità di essere salvati su più piattaforme
- Disponibili sempre lungo tutto il loro ciclo di vita

Per questo motivo un sistema SCADA+Historian che raccolga e storicizzi dati, informazioni ed eventi su impianti e macchine di produzione batch e continua è caldamente consigliato per non incorrere in problematiche di conformità e avere sotto controllo tutti i dati, per una data integrity a prova di errore.

DATA INTEGRITY AND COMPLIANCE WITH DRUG CGMP