Webinar com a Gerência de Inspeção e Fiscalização de Medicamentos e Insumos Farmacêuticos sobre Consultas Públicas Internacionais do PIC/S

Realização:

Gerência de Inspeção e Fiscalização de Medicamentos e Insumos Farmacêuticos – GIMED
Gerência-Geral de Inspeção e Fiscalização Sanitária – GGFIS

Agência Nacional de Vigilância Sanitária

Consultas públicas internacionais do PIC/S

ANVISA
Agência Nacional de Vigilância Sanitária

AGENDA

- **Annex 11 — Sistemas computadorizados -** IN 134/2022
- **Annex 22 – INTELIGÊNCIA ARTIFICIAL –** Novo
- **Chapter 4 – DOCUMENTAÇÃO -** Capítulo V da RDC 658/2022
- **Chapter 1 - SISTEMA DA QUALIDADE FARMACÊUTICA -** Capítulo II da RDC 658/2022

ANVISA
Agência Nacional de Vigilância Sanitária

AGENDA

- **Draft Annex 11 — Sistemas computadorizados**

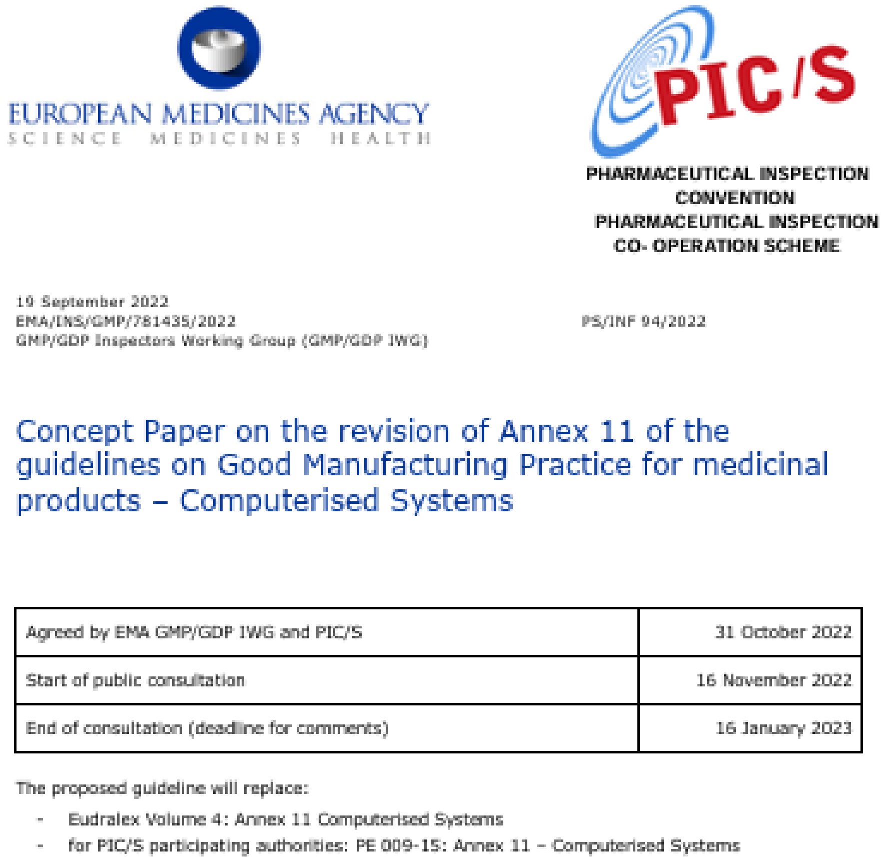
DRAFT - ANNEX 11

Publicação do Concept Paper

2022 - Primeira visão do escopo esperado para a nova regulamentação

Grupo de Trabalho EMA GMP/GDP IWG and PIC/S

Melhoria Estrutural



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO- OPERATION SCHEME

19 September 2022
EMA/INS/GMP/781435/2022
GMP/GDP Inspectors Working Group (GMP/GDP IWG)

PS/INF 94/2022

Concept Paper on the revision of Annex 11 of the guidelines on Good Manufacturing Practice for medicinal products – Computerised Systems

Agreed by EMA GMP/GDP IWG and PIC/S	31 October 2022
Start of public consultation	16 November 2022
End of consultation (deadline for comments)	16 January 2023

The proposed guideline will replace:

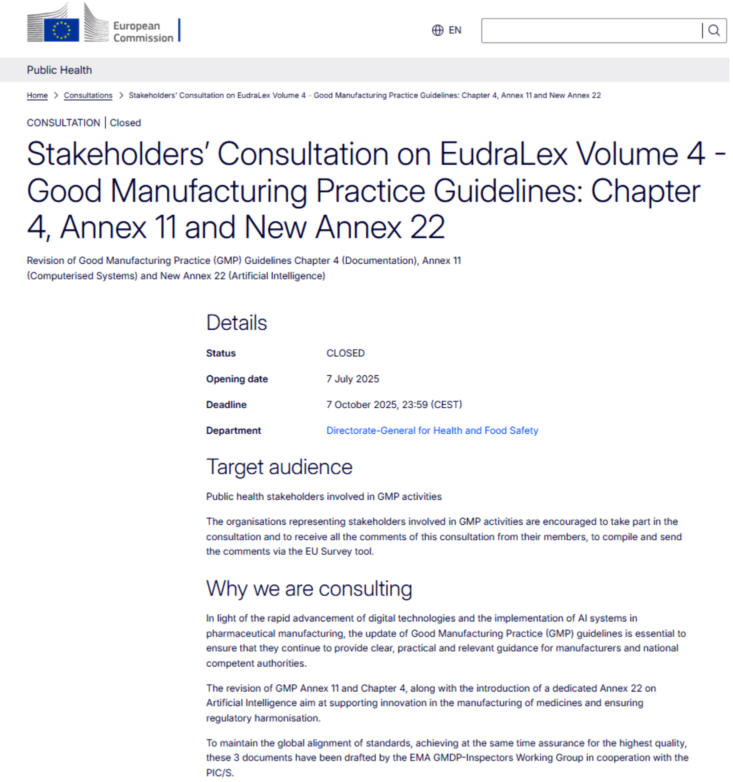
- Eudralex Volume 4: Annex 11 Computerised Systems
- for PIC/S participating authorities: PE 009-15: Annex 11 – Computerised Systems

DRAFT ANNEX 11 – CONSULTA PÚBLICA

- Consulta pública internacional – julho de 2025 (3 meses)
- Aumenta o escopo – medicamentos e insumos farmacêuticos

<u>Brasil</u>

- Ofício às entidades ligadas a indústria farmacêutica e ao SNVS
- Publicação de notícia no site da Anvisa



European Commission
EN
Public Health
Home > Consultations > Stakeholders' Consultation on EudraLex Volume 4 - Good Manufacturing Practice Guidelines: Chapter 4, Annex 11 and New Annex 22

CONSULTATION | Closed

Stakeholders' Consultation on EudraLex Volume 4 - Good Manufacturing Practice Guidelines: Chapter 4, Annex 11 and New Annex 22

Revision of Good Manufacturing Practice (GMP) Guidelines Chapter 4 (Documentation), Annex 11 (Computerised Systems) and New Annex 22 (Artificial Intelligence)

Details

Status	CLOSED
Opening date	7 July 2025
Deadline	7 October 2025, 23:59 (CEST)
Department	Directorate-General for Health and Food Safety

Target audience

Public health stakeholders involved in GMP activities

The organisations representing stakeholders involved in GMP activities are encouraged to take part in the consultation and to receive all the comments of this consultation from their members, to compile and send the comments via the EU Survey tool.

Why we are consulting

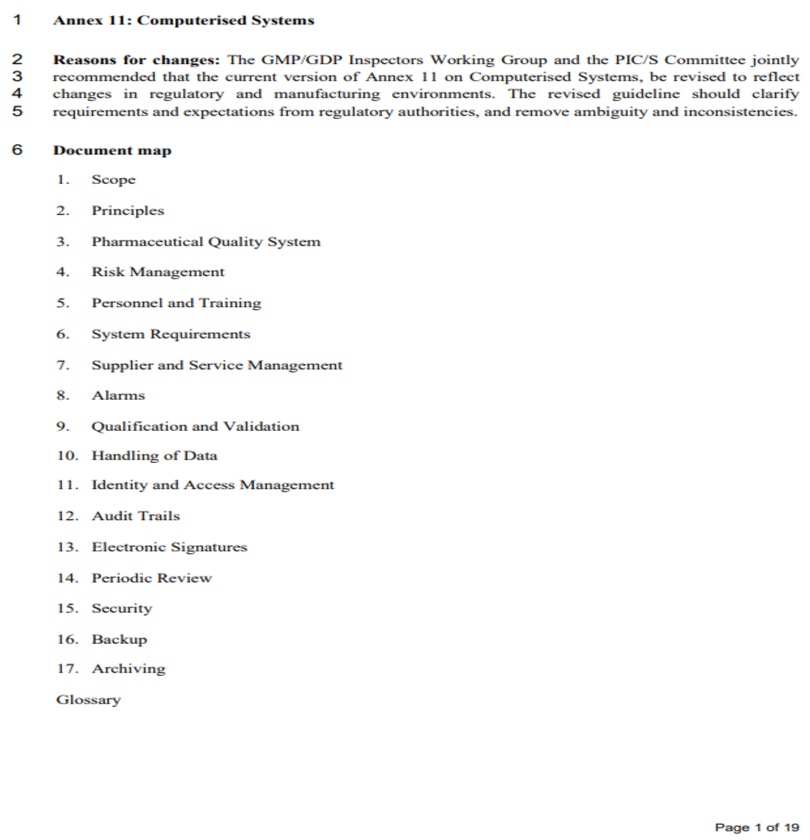
In light of the rapid advancement of digital technologies and the implementation of AI systems in pharmaceutical manufacturing, the update of Good Manufacturing Practice (GMP) guidelines is essential to ensure that they continue to provide clear, practical and relevant guidance for manufacturers and national competent authorities.

The revision of GMP Annex 11 and Chapter 4, along with the introduction of a dedicated Annex 22 on Artificial Intelligence aim at supporting innovation in the manufacturing of medicines and ensuring regulatory harmonisation.

To maintain the global alignment of standards, achieving at the same time assurance for the highest quality, these 3 documents have been drafted by the EMA GMDP-Inspectors Working Group in cooperation with the PIC/S.

DRAFT ANNEX 11 – ESTRUTURA E ORGANIZAÇÃO

- 17 seções expandidas + glossário extenso
- 19 páginas
- Estrutura mais elaborada com subseções numeradas
- Documento mais prescritivo e detalhado
- Transformação digital



Annex 11: Computerised Systems

Reasons for changes: The GMP/GDP Inspectors Working Group and the PIC/S Committee jointly recommended that the current version of Annex 11 on Computerised Systems, be revised to reflect changes in regulatory and manufacturing environments. The revised guideline should clarify requirements and expectations from regulatory authorities, and remove ambiguity and inconsistencies.

Document map

Page 1 of 19

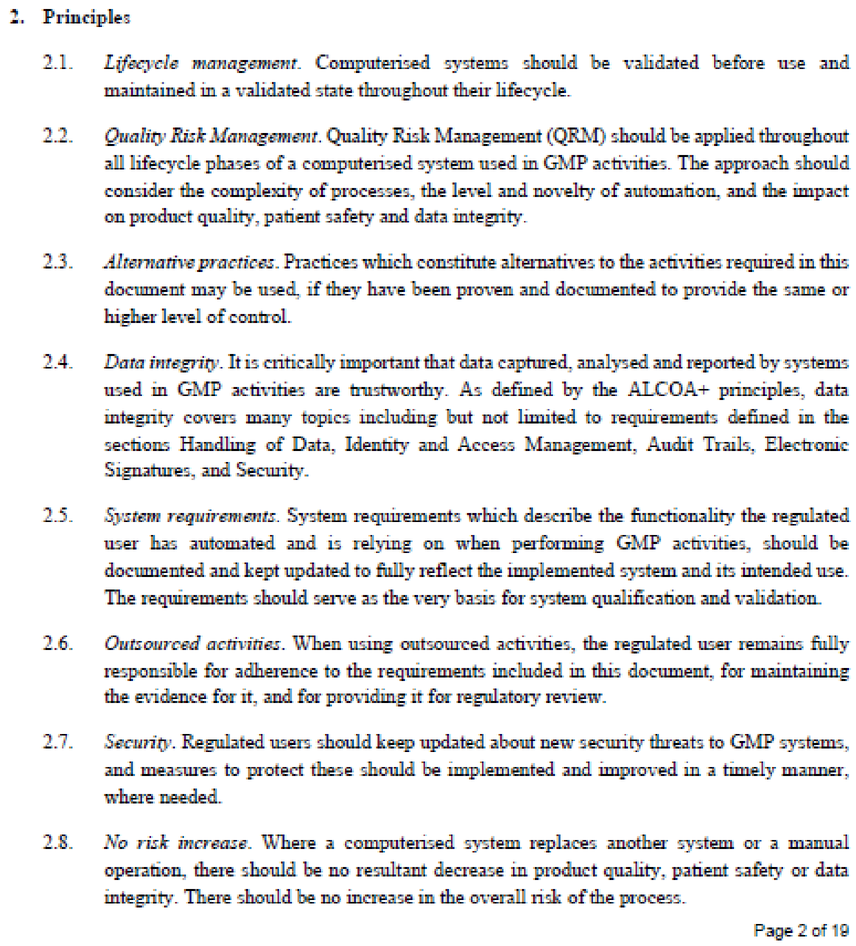
ANVISA
Agência Nacional de Vigilância Sanitária

DRAFT ANNEX 11 – PRINCIPLES

Data integrity: ALCOA+ (*Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available*)

System requirements: Qualification/Validation

No risk increase



2. Principles

2.1. *Lifecycle management*. Computerised systems should be validated before use and maintained in a validated state throughout their lifecycle.

2.2. *Quality Risk Management*. Quality Risk Management (QRM) should be applied throughout all lifecycle phases of a computerised system used in GMP activities. The approach should consider the complexity of processes, the level and novelty of automation, and the impact on product quality, patient safety and data integrity.

2.3. *Alternative practices*. Practices which constitute alternatives to the activities required in this document may be used, if they have been proven and documented to provide the same or higher level of control.

2.4. *Data integrity*. It is critically important that data captured, analysed and reported by systems used in GMP activities are trustworthy. As defined by the ALCOA+ principles, data integrity covers many topics including but not limited to requirements defined in the sections Handling of Data, Identity and Access Management, Audit Trails, Electronic Signatures, and Security.

2.5. *System requirements*. System requirements which describe the functionality the regulated user has automated and is relying on when performing GMP activities, should be documented and kept updated to fully reflect the implemented system and its intended use. The requirements should serve as the very basis for system qualification and validation.

2.6. *Outsourced activities*. When using outsourced activities, the regulated user remains fully responsible for adherence to the requirements included in this document, for maintaining the evidence for it, and for providing it for regulatory review.

2.7. *Security*. Regulated users should keep updated about new security threats to GMP systems, and measures to protect these should be implemented and improved in a timely manner, where needed.

2.8. *No risk increase*. Where a computerised system replaces another system or a manual operation, there should be no resultant decrease in product quality, patient safety or data integrity. There should be no increase in the overall risk of the process.

Page 2 of 19

DRAFT ANNEX 11 – PHARMACEUTICAL QUALITY SYSTEM

3.1. *Pharmaceutical quality system. A regulated user should implement a pharmaceutical quality system (PQS),* ***which covers all computerised systems used in GMP activities and personnel involved with these***.

- Registro de desvios e investigação de causa raiz
- CAPA (Corrective and Preventive Actions)
- *Change control* robusto
- Auditorias internas
- *Management reviews* com KPIs
- Supervisão da alta gestão (*senior management oversight*)

DRAFT ANNEX 11 – RISK MANAGEMENT

4.5. Data integrity. Quality risk management principles should be used to assess the ***criticality of data*** *to product quality, patient safety and data integrity,* ***the vulnerability*** *of data to deliberate or indeliberate alteration, deletion or loss, and the* ***likelihood of detection*** *of such actions.*

CRITICIDADE (Impacto)

↓

[ALTO/BAIXO]

↓

VULNERABILIDADE ←→ DETECTABILIDADE

(Facilidade de alterar/perder) (Probabilidade de detectar)

↓

RISCO DE INTEGRIDADE

↓

[Definir controles apropriados]

DRAFT ANNEX 11 – PERSONNEL AND TRAINING

5.1 Cooperation. When conducting the activities required in this document, there should be, where applicable, close cooperation between all relevant parties. This includes **process owner, system owner, users, subject matter experts (SME), QA, QP, the internal IT department, vendors, and service providers**.

5.2. *Training*. All parties involved with computerised systems used in GMP activities **should have adequate system specific training**, and appropriate qualifications and experience, corresponding to their **assigned responsibilities, duties and access privileges**.

DRAFT ANNEX 11 – ALARMS

TÓPICO NOVO

8.1 Reliance on system: *This is required when the user must take a specific action, without which product quality, patient safety or data integrity might otherwise be compromised.*

8.2 Settings: *Alarm limits, delays, and any early warnings or alerts, should be appropriately justified, and set within approved and validated process and product specifications*

8.3 Signalling: *Alarms should set off visible and/or audible signals when set alarm limits are exceeded and after any defined delay.*

8.4 Acknowledgement: Critical alarms potentially impacting product quality, patient safety or data integrity should only be acknowledged by users with appropriate access privileges.

DRAFT ANNEX 11 – ALARMS

TÓPICO NOVO

8.5 Log: *All alarms and acknowledgements should be automatically added to an alarm log.*

8.6 Searchability: *Alarm logs should be searchable and sortable.*

8.7 Review: *Alarm logs should be subject to appropriate periodic reviews based on approved procedures, in which it should be evaluated whether they have been timely acknowledged by authorised users and whether appropriate action has been taken.*

DRAFT ANNEX 11 – HANDLING OF DATA

10.1. *Input verification*. Where critical data is entered manually, systems should, were applicable, have functionality to verify the plausibility of the inputs (e.g. within expected ranges), and alert the user when the input is not plausible.

10.2. *Data transfer*. [...] If critical data is transcribed manually, effective measures should be in place to ensure that this does not introduce any risk to data integrity.

10.3. Data migration. Where an ad hoc **process requires that critical data or a whole database be migrated from one system to another** (e.g. when moving data from a retired to a new system), this should be based on a validated process. Among other things, it should consider the constraints on the sending and receiving side.

10.4. *Encryption*. Where applicable, critical data should be encrypted on a system.

DRAFT ANNEX 11 – IDENTITY AND ACCESS MANAGEMENT

11.1. *Unique accounts*. All users should **have unique and personal accounts.** The use of **shared accounts** except for those limited to read-only access (no data or settings can be changed), **constitute a *violation* of data integrity**.

11.3. *Certain identification*. **The method of authentication should identify users with a high degree of certainty and provide an effective protection against unauthorised access**. Typically, it may involve a unique username and a password, although other methods providing at least the same level of security may be employed (e.g. biometrics). **Authentication only by means of a token or a smart card is not sufficient**, if this could be used by another user.

DRAFT ANNEX 11 – IDENTITY AND ACCESS MANAGEMENT

11.4 Confidential passwords. Passwords and other means of authentication **should be kept confidential and protected from all other users**, both at system and at a personal level. Passwords received from e.g. a manager, or a system administrator should be changed at the first login, preferably required by the system.

11.5 Secure passwords. Passwords should be secure and enforced by systems**. Password rules should be commensurate with risks and consequences of unauthorised changes in systems and data. For critical systems, passwords should be of sufficient length to effectively prevent unauthorised access** and contain a combination of uppercase, lowercase, numbers and symbols. A password should not contain e.g. words that can be found in a dictionary, the name of a person, a user id, product or organisation, and should be significantly different from a previous password.

DRAFT ANNEX 11 – IDENTITY AND ACCESS MANAGEMENT

11.7. *Auto locking*. **Accounts should be automatically locked after a pre-defined number of successive failed authentication attempts.** Accounts should only be unlocked by the system administrator after it has been confirmed that this was not part of an unauthorised login attempt or after the risk for such attempt has been removed.

11.9. *Access log*. **Systems should include an access log**(separate, or as part of the audit trail) **which, for each login, automatically logs the username, user role**(if possible, to choose between several roles), **the date and time for login, the date and time for logout** (incl. inactivity logout). **The log should be sortable and searchable**, or alternatively, it should be possible to export the log to a tool which provides this functionality.

DRAFT ANNEX 11 – IDENTITY AND ACCESS MANAGEMENT

11.10. *Guiding principles*. **Access privileges** for users of computerised systems used in GMP activities **should be managed according to** the following two guiding principles:

•Segregation of duties, i.e. that users who are involved in GMP activities do not have administrative privileges.
•Least privilege principle, i.e. that users do not have higher access privileges than what is necessary for their job function.

11.8. *Inactivity logout*. **Systems should include an automatic inactivity logout**, **which logs out a user after a defined period of inactivity**. The user should not be able to change the inactivity logout time(outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a re-authentication should be required(e.g. password entry).

DRAFT ANNEX 11 – IDENTITY AND ACCESS MANAGEMENT

11.11. *Recurrent reviews.* **User accounts should be subject to recurrent reviews where managers confirm the continued access of their employees** in order to detect accesses which should have been changed or revoked during daily operation, but were accidentally forgotten. If user accounts are managed by means of roles, these should be subject to the same kind of reviews, where the accesses of roles are confirmed. The reviews should be documented, and appropriate action taken. The frequency of these reviews should be commensurate with the risks and consequences of changes in systems and data made by unauthorised individuals.

DRAFT ANNEX 11 – ELECTRONIC SIGNATURES

13.3. *Re-authentication*. When executing an electronic signature, a system should enforce users to perform a **full re-authentication providing at least the same level of security as during system login** (see 11.3 Certain identification). When executing subsequent electronic signatures in immediate sequence, authentication may be by means of a password or biometrics only. *Authentication only by means of a smart card, a pin code*, or relying on the previous system authentication is not acceptable.

13.8. *Unbreakable link*. **Electronic signatures should be permanently linked to their respective records**. Controls should be in place to ensure that a **signed record cannot be modified or alternatively, that if a later change is made to a signed record, it will clearly appear as unsigned.**

DRAFT ANNEX 11 – AUDIT TRAIL

Audit trail passou de OPCIONAL baseado em risco (*"considerations should be given"*) para OBRIGATÓRIO!

12.1. *Manual user interactions*. Systems which are used to control processes, capture, hold or report data, and where users can create, modify or delete data, settings or access privileges, acknowledge alarms or execute electronic signatures etc., **should have an audit trail functionality which automatically logs all manual user interactions**.

12.2. ***Who, what, when, why***. The audit trail should unambiguously capture the user who made a change (including the user's role, if users may have more than one role), what was changed (including the data that was changed and the old and the new value), and the date and time when the change was made (including the time zone if applicable). Audit trail data should be recorded at the time of events, not at the end of a process. Where data is changed from an old value to a new value, systems should automatically prompt the user for, and register the reason, why the change was made.

DRAFT ANNEX 11 – AUDIT TRAIL

12.3. *No edit or deactivation.* Audit trail functionality should be enabled and locked at all times, and it should **not be possible for any** user to edit audit trail data. If audit trail settings or system time can be changed, or **if the functionality can be deactivated, this should by itself create an entry in the audit trail, and it should only be possible for a system administrator not involved in any GMP activities**(see 11.10 Guiding principles).

12.5. *Reviews.* **Audit trail reviews should be conducted according to a documented procedure for the specific system**, or type of systems. The procedure should outline **who should make the review, what should be reviewed, and when should the review be made.** The use of tools to help conduct audit trail reviews is encouraged and appropriate action should be taken and documented following the reviews. Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded.

DRAFT ANNEX 11 – AUDIT TRAIL

12.7. *Scope of review.* Reviewing all entries in an audit trail record may not be effective. **Reviews should be targeted, based on risk and adapted to local manufacturing processes**. Procedures for audit trail reviews should **focus on detecting any deliberate or indeliberate changes to critical processes** or data that indicate a violation of GMP principles, including, but not limited to, repetition of activities, errors, omissions, unauthorised process deviations and loss of data integrity. **A key element should be to verify the reason why a change is made**.

DRAFT ANNEX 11 – BACKUP

16.1. *Regular backup.* **Data and metadata should be regularly backed up following established procedures to prevent the loss of data** in case of accidental or deliberate change or deletion, loss as the result of a malfunction or corruption, e.g. as the result of a cyber-attack.

16.2. *Frequency and retention*. **The frequency, retention period and storage of backups** is critically **important to the effectiveness of the process to mitigate the loss of data**. Backups should be made at suitable intervals(e.g. hourly, daily, weekly and monthly) and their retention determined through a risk-based approach(e.g. correspondingly a week, a month, a quarter, and years).

DRAFT ANNEX 11 – BACKUP

16.5. *Scope*. Depending on the criticality and urgency for recovery after an incident, applications and system configurations may also need to be backed up.

16.4. *Physical separation*. **Backups should be physically separated from the server or computer holding the original data and stored at a safe distance** from this, to prevent that both would be impacted by the same incident.

16.3. *Logical separation*. **Backups should not be stored at the same logical network as the original data to avoid simultaneous destruction or alteration**.

16.6. *Restore test*. **Restore of data from backup should be tested and documented based on risk during system validation and after changes** are made to the backup or restore processes and tools. Restore tests should be documented and include a verification that data is accessible on the system.

ANVISA
Agência Nacional de Vigilância Sanitária

DRAFT ANNEX 11 – SECURITY

15.4. *Physical access.* **Servers, computers, devices, infrastructure and storage media used in GMP activities should be physically protected against unauthorised access, damage and loss.** Physical access to server rooms and data centres should be limited to the necessary minimum and these should be securely locked, e.g. by means of multi-factor authentication. **If unauthorised access is possible (e.g. `co-location´), access to individual servers should be protected.**

11.6. *Strong authentication.* **Remote authentication on critical systems from outside controlled perimeters, should include multifactor authentication (MFA).**

15.20. *Encryption.* **When remotely connecting to systems over the internet, a secure and encrypted protocol should be used**.

DRAFT ANNEX 11 – SECURITY

15.8. *Segmentation and firewalls*. **Networks should be segmented**, and **effective firewalls implemented to provide barriers between networks, and control incoming and outgoing network traffic.** Firewall rules (e.g. based on IP addresses, destinations, protocols, applications, or ports) should be defined as strict as practically feasible, only allowing necessary and permissible traffic.

15.9. *Review of firewalls*. **Firewall rules should be periodically reviewed** as the rules tend to be changed or become insufficient over time (e.g. as ports are opened but never closed, or as new cyber threats evolve). This review should ensure that firewalls continue to be set as tight as possible.

15.10. *Updated platforms*. Operating systems and **platforms for applications should be updated in a timely manner according to vendor recommendations**, to prevent their use in an unsupported state.

15.11. *Validation and migration*. **Validation of applications on updated operating systems and platforms and migration of data should be planned** and completed in due time prior to the expiry of the vendor's support.

DRAFT ANNEX 11 – SECURITY

15.13. *Timely patching*. While operating systems and platforms are under support, vendors typically release security patches to counter identified vulnerabilities, some of which (critical vulnerabilities) could otherwise be exploited to give unauthorised individuals privileged access to systems and allow code execution (e.g. ransomware attacks). Hence, **relevant security patches released by vendors of operating systems and platforms should be deployed in a timely manner according to vendor recommendations**. For critical vulnerabilities, this might be immediately.

15.15. *Strict control*. **The use of bidirectional devices** (e.g. USB) **in servers and computers used in GMP activities should be strictly controlled within the organisation**.

15.16. *Effective scan*. If bidirectional devices (e.g**. USB**) may have been used outside the organisation (e.g. privately), they may intentionally or unintentionally introduce malware and cause code execution. Hence, they should not be used unless they have been **effectively scanned and found to be harmless, and not compromise system and data integrity.**

ANVISA
Agência Nacional de Vigilância Sanitária

DRAFT ANNEX 11 – ARCHIVING

17.1. *Read only.* **After completion of a process, e.g. release of a product, GMP data and metadata (incl. audit trails) should be protected from deletion and changes throughout the retention period.** This may be by changing its status to read-only in the system where the data was generated or captured, or by moving it to a dedicated archival system via a validated interface.

17.3. *Backup*. If data is archived on a server (disk), it should be regularly backed up following the same procedures as for live data (see 16 Backup). As for other backups, these should be physically and logically separated from the archived data.

17.5. ***Retrieval*. It should be possible to retrieve archived data and metadata in a format which allows searching and sorting of the data**, or alternatively, to allow export of the data to a tool where this is possible.

REFERÊNCIAS

PIC/S: https://picscheme.org/en/publications?tri=all#zone

DÚVIDAS: chat P&R