



MANUAL

# BOAS PRÁTICAS REGULAMENTARES

Ordem dos Farmacêuticos

---

# 11

## ***BUSINESS CONTINUITY***

### **AUTORIA**

Ana Rita Parcerias Simões Caramelo  
Dina Teresa Gomes Duarte Caldeira

### **COMISSÃO CIENTÍFICA**

Maria Teresa da Silva Pinto Ribeiro de Carvalho

### **COMISSÃO EXECUTIVA**

Fernanda Maria Gonçalves Aragão Aleixo (*presidente*)  
Ana Sofia Araújo Ganhão de Oliveira  
Carla Cristina Fernandes Gomes (*até 2022*)  
Dinah da Conceição Marçal Verdugo Duarte (*a partir de 2022*)  
Filipa Sameiro de Oliveira  
Leila Carina do Rosário Sousa Fernandes Almeida (*a partir de 2022*)  
Maria Teresa da Silva Pinto Ribeiro de Carvalho (*a partir de 2022*)  
Marília Cândida Pinto de Noronha  
Paula Cristina Carvalho Sanches Dias

## A. OBJETIVO E ÂMBITO

O objetivo deste capítulo é descrever sumária e esquematicamente, as ações conducentes à definição, desenvolvimento e aplicação de um plano de continuidade de negócio (*Business Continuity Plan* - BCP) a todas as áreas técnicas de uma organização.

Com base numa análise de impacto empresarial, será fundamental identificar as funções e processos críticos para a sobrevivência da organização, definir a estratégia de recuperação da mesma, em situações de acontecimentos críticos ou disruptivos, tais como catástrofes regionais e/ou mundiais, que possam comprometer as suas infraestruturas, os recursos humanos, tecnológicos e outros, e o seu regular funcionamento.

Este documento pretende ser um guia prático para o desenvolvimento de um plano de continuidade, abordando os meios e sistemas de segurança de informação (*backups*), procedimentos a cumprir e condutas a adotar para garantir a continuidade operacional da organização.

Paralelamente, assegurar a manutenção e eficiência dos fluxos de informação e operacionalidade, entre as organizações congéneres, academia, autoridades competentes, e demais organizações, nas áreas de investigação (incluindo ensaios clínicos), regulamentar e de farmacovigilância, e outras consideradas fulcrais. Poderá ser aplicável em situações de urgência, emergência, disruptivas, como por exemplo, as que ocorrem após catástrofes naturais, com cenários de inundação, neve, terramoto, incêndio, ou em pandemia, ameaça química, biológica, informática ou de outra causa.

## B. INTRODUÇÃO

Na ISO 22301, o BCP ou Plano de Continuidade de Negócio é descrito como a capacidade da organização em continuar a prestar os produtos e serviços a níveis predefinidos aceitáveis, após um acontecimento disruptivo. A Gestão da Continuidade do Negócio (GCN) envolve a recuperação e continuidade das atividades do negócio no caso de uma rutura, bem como a gestão de um programa geral que inclui formação, exercícios e revisões, para assegurar a permanente atualização do BCP.

Toda e qualquer organização pública ou privada, oficial ou não, que no âmbito das suas atividades e competências, tenha na sua área de intervenção, a gestão de uma ou mais unidades funcionais, definidas como áreas *core* para a manutenção do negócio, deverá ter implementado um sistema de gestão de risco que inclua cada uma dessas atividades.

Como parte integrante e fundamental desse sistema de gestão de risco, existirá uma matriz de responsabilidades, e contactos operacionais, definidos para as atividades de rotina, mas em particular para a eventual gestão de uma situação de crise. Para que este modelo de atuação possa operar, são necessários alguns princípios dos quais destacamos:

- » **Comprometimento da gestão de topo (DG/ADM/Tutela)** - de modo a assegurar todos os recursos humanos, tecnológicos e outros meios necessários para que sejam garantidas

e mantidas as condições de operabilidade das organizações, em todos os cenários possíveis, incluindo os de catástrofe ou pandemia.

- » **Disponibilidade de equipa de STI** - de modo a assegurar um “Espaço de Trabalho Digital Seguro”, meios tecnológicos e procedimentos adequados que permitam trabalhar remotamente, fazer cópias de segurança de informação *core* da organização e simultaneamente proceder à recuperação dessa informação *core* armazenada, e dispor dela de forma expedita e útil, no caso de falha pontual, prolongada ou em cenário disruptivo. Proceder ainda à validação das opções tecnológicas escolhidas, para efeitos de eventual auditoria ou ação inspetiva, em termos legais e de proteção de dados.
- » **Garantir em permanência rotativa colaboradores “chave” nomeados pela ADM/DG/Tutela** - que possam tomar decisões, e monitorizar à distância, a implementação de planos de contingência para os processos críticos, em situações de falha prolongada, devido a eventos disruptivos, tais como catástrofe, pandemia ou outros. Os responsáveis mandatados devem periodicamente reavaliar a pertinência e viabilidade dos meios colocados à sua disposição.

O plano de continuidade de negócio é um documento que descreve como uma área ou organização vai gerir um acontecimento negativo que coloca em perigo a continuidade do negócio. Este consiste num procedimento escrito, atualizado, treinado, sendo importante para identificar potenciais riscos e que ajuda a assegurar o negócio e a ultrapassar o acontecimento negativo, bem como que área/organização assegura a resposta aos seus clientes internos e externos, minimizando o risco para o negócio.

## C.

### DESENVOLVIMENTO, APROVAÇÃO E MANUTENÇÃO DE UM BCP

Para desenvolver um BCP podem ser seguidos os seguintes 6 passos:

#### C.1 PRIMEIRO PASSO

Na fase inicial deve ser determinado porque é necessário um BCP, qual o âmbito do mesmo, as áreas abrangidas, e ser nomeado um responsável pelo BCP e a equipa de trabalho para a elaboração do plano. No caso de empresas multinacionais, deverá ainda ser averiguada a existência de um BCP da organização para cada área específica e implementado, se aplicável. O BCP da área específica deverá estar alinhado e incorporado no BCP geral da organização, caso exista.

O responsável da área deve assegurar a existência e manutenção de planos de contingência aplicáveis a cada um dos setores afetados que devem estar em linha com os da organização, caso existam. Devem ainda assegurar a existência de meios e procedimentos adequados que permitam fazer a sua execução, como por exemplo, fazer backup e recuperação da informação e operacionalidade desses meios, em qualquer cenário extremo em que se aplique.

## C.2 SEGUNDO PASSO

Na fase inicial deve ser determinado porque é necessário um BCP, qual o âmbito do mesmo, as áreas abrangidas, e ser nomeado um responsável pelo BCP e a equipa de trabalho para a elaboração do plano. No caso de empresas multinacionais, deverá ainda ser averiguada a existência de um BCP da organização para cada área específica e implementado, se aplicável. O BCP da área específica deverá estar alinhado e incorporado no BCP geral da organização, caso exista.

## C.3 TERCEIRO PASSO

Após a análise, devem ser desenvolvidas as estratégias para minimizar os riscos de o acontecimento negativo para a área/organização responder à interrupção da atividade, assegurando a *compliance* regulamentar e recuperar a atividade após o acontecimento ou durante o acontecimento.

## C.4 QUARTO PASSO

A informação anterior é então documentada no BCP, identificando os potenciais riscos para o negócio/atividade e como minimizar e recuperar do acontecimento negativo de forma a manter a *compliance* regulamentar, a continuidade do negócio, responder aos clientes e autoridades, e garantir o contínuo fornecimento dos medicamentos e produtos de saúde, tendo como base o pior cenário possível, podendo também incluir acontecimentos negativos menos críticos.

Exemplos de informação a incluir no BCP:

- » Responsável do BCP;
- » Descrição dos processos críticos essenciais e não essenciais, bem como as atividades prioritárias e não prioritárias para a área, lista de contactos essenciais (nome, cargo, telefone, endereço eletrónico) em rede e em papel de forma a manter o contacto entre os colaboradores da área, organização interna e externos;
- » Localização de instalações alternativas com material informático (por exemplo computadores, impressoras) e com acesso à rede e a um telefone fixo e/ou telemóvel;
- » Disponibilização adicional do material informático de outros colaboradores que na referida situação (por exemplo da força de vendas), não estejam a operar;
- » Periodicidade de *backups* informáticos (sendo aconselhável que por sistema, o arquivo informático preferencialmente já seja em rede, em vez de no próprio computador) e sua reposição;
- » *Backups* de determinadas funções ou de colaboradores;
- » Arquivo de documentos originais críticos em armários/salas “corta-fogo”;
- » Digitalização em rede;
- » Implementação de assinaturas digitais;
- » Níveis de aprovações ad hoc e simplificadas.

O BCP deve descrever o processo relativo à sua ativação, nomeadamente como é ativado, e os responsáveis por essa ativação, o procedimento que o responsável deve adotar nesta decisão, os colaboradores que devem ser consultados antes e após a desta decisão ser tomada, quem vai para onde e quando, que serviços estarão disponíveis e mobilização de recursos, comunicação desta informação, se relevante, procedimentos detalhados para soluções manuais, recuperação dos sistemas etc.

Deverá ser também incluído um documento *template* onde deverão ser registados e documentados todos os desvios aos procedimentos e às normas vigentes na área/organização durante o período do BCP para posterior correção, memória futura (tal como para auditorias e autoinspeções) bem como para melhorar as normas e processos, incluindo o próprio BCP.

A área/organização deverá ser ágil, flexível e simplificar procedimentos durante o acontecimento negativo, restringindo-se ao essencial até à recuperação do estado de normalidade.

## C.5 QUINTO PASSO

A fase seguinte do desenvolvimento de um BCP, inclui testar os procedimentos descritos no BCP, o que deve ser realizado periodicamente de forma a garantir a sua exequibilidade e treino dos colaboradores. Por exemplo pode ser realizado anualmente ou de dois em dois anos (conforme for considerado no BCP), um simulacro de um evento negativo ou se se verificar uma alteração significativa na organização.

## C.6 SEXTO PASSO

A última fase do desenvolvimento do BCP consiste na sua contínua melhoria. Assim, com base nas conclusões retiradas do simulacro, de qualquer outro teste ou de acontecimento negativo real, bem como de uma alteração legislativa ou alteração significativa da organização, o BCP deve ser atualizado e melhorado em conformidade.

O BCP deve ser aprovado pelo responsável da área e da organização relevantes, deverá ser distribuído e arquivado. O BCP, deverá estar facilmente acessível em formato informático e em papel, em caso de ocorrência de um acontecimento negativo. Os colaboradores da área devem receber formação periódica sobre o BCP, pelo menos sempre que este for revisto.

Adicionalmente podem ser desenvolvidos BCP específicos para um acontecimento crítico que possa afetar a determinada área ou negócio, como a continuidade de abastecimento doo medicamentos e produtos ao mercado, nomeadamente no seu pior cenário, devido ao aumento do volume de trabalho que tal acontecimento irá originar, devido à sua incerteza, calendário de implementação, etc.

São exemplos destes potenciais eventos, na área regulamentar do medicamento, a alteração do nome do Titular de AIM, transferência de local de fabrico ou libertação de lotes, a mudança de instalações, implementação de uma nova legislação, pandemias que afetem autoridades competentes e vários *stakeholders*.

A última fase do desenvolvimento do BCP consiste na sua contínua melhoria. Assim, com base

nas conclusões retiradas do simulacro, de qualquer outro teste ou de acontecimento negativo real, bem como de uma alteração legislativa ou alteração significativa da organização, o BCP deve ser atualizado e melhorado em conformidade. Sendo o BCP um documento dinâmico, este deverá ser revisto periodicamente. Esta revisão periódica, deve estar descrita no BCP.

O BCP deve ser aprovado pelo responsável da área e da organização relevantes, deverá ser distribuído e arquivado. O BCP, deverá estar facilmente acessível em formato informático e em papel, em caso de ocorrência de um acontecimento negativo. Os colaboradores da área devem receber formação periódica sobre o BCP, pelo menos sempre que este for revisto.

Adicionalmente podem ser desenvolvidos BCP específicos para um acontecimento crítico que possa afetar a determinada área ou negócio, como a continuidade de abastecimento doo medicamentos e produtos ao mercado, nomeadamente no seu pior cenário, devido ao aumento do volume de trabalho que tal acontecimento irá originar, devido à sua incerteza, calendário de implementação, etc.

São exemplos destes potenciais eventos, na área regulamentar do medicamento, a alteração do nome do Titular de AIM, transferência de local de fabrico ou libertação de lotes, a mudança de instalações, implementação de uma nova legislação, pandemias que afetem autoridades competentes e vários *stakeholders*.

## D.

### ESPECIFICIDADES A CONSIDERAR PELA AUTORIDADE COMPETENTE

Também do lado das Autoridade Competentes deve ser definido, elaborado e testado um BCP.

As autoridades competentes devem, à semelhança das empresas, definir quais as áreas e processos críticos que devem ser assegurados em caso de evento disruptivo.

Entre outras, são atribuições das autoridades competentes a promoção e proteção da saúde pública e/ou animal e a regulação e supervisão das atividades de investigação, produção, distribuição, comercialização e utilização, garantindo o acesso a produtos de qualidade, eficazes e seguros.

Do ponto de vista da autoridade, numa situação em que as atividades habituais das autoridades competentes possam ser comprometidas (elevada rotatividade de recursos humanos, pandemias, catástrofes ambientais, mudança de instalações, falhas tecnológicas, ataque informático) o BCP deve permitir que as atividades *core* sejam mantidas de forma a garantir a salvaguarda e proteção da saúde pública e/ou animal.

Alguns exemplos de atividades que poderão ser comprometidas/reduzidas/suspensas, ou adiadas durante o acontecimento negativo, e para as quais é necessário o planeamento prévio e adaptação poderão ser:

- » Integração e participação na rede regulamentar europeia e colaboração a nível internacional: cooperação institucional, cooperação com os Estados Membros, etc.;
- » Desenvolvimento de *guidelines*, orientações, instruções aos requerentes, Q&A (envolvimento na evolução legislativa, na formulação da política de saúde) sobre áreas terapêuti-

cas fundamentais (antibioterapia)

- » Programas e projetos (programas no âmbito de determinadas patologias ou acesso a medicamentos, projetos com farmácias comunitárias; com universidades e outras instituições de investigação e desenvolvimento);
- » Interação com *stakeholders* (reuniões, eventos, sessões de esclarecimento);
- » Reunião de comissões, comités, grupos.

Por outro lado, as atividades ligadas relacionadas ao evento poderão o aumentar, por exemplo “orientações” relativas a vacinas para a uma pandemia, listagem de fármacos essenciais, sistemas de suporte de vida, etc.

## G.

### ESPECIFICIDADES A CONSIDERAR PARA A ÁREA DE FARMACOVIGILÂNCIA

Atendendo às especificidades da área da Farmacovigilância, será necessário garantir a disponibilidade de equipas de STI que possibilitem a continuidade de um “Espaço de Trabalho Digital Seguro” com meios tecnológicos validados e procedimentos técnicos adequados que permitam efetuar sem interrupção, o trabalho remoto, realizar *backups* e recuperação da informação do Sistema de Farmacovigilância armazenada nos servidores da organização. Torna-se por isso fundamental, apoiar tecnologicamente, os intervenientes diretos e indiretos afetos ao Sistema de Farmacovigilância, nomeadamente QPPV, QPPV *deputy*, e outros nomeados para acederem à informação para cumprimento das obrigações de notificação às autoridades competentes, demais organizações, e entidades identificadas no SDEA aplicável. A permanência funcionante dos colaboradores nomeados, incluindo os da CRO, é crítica para garantir que o plano de contingência para o Sistema de Farmacovigilância, é acionado em situações de falha, e poderá ser monitorizado e coordenado à distância, permitindo o funcionamento e a supervisão de todas as tarefas que estão atribuídas ou subcontratadas caso seja aplicável.

Principais pontos a considerar num BCP para a área da Farmacovigilância, aplicáveis também à área regulamentar:

- » Os colaboradores afetos ao Sistema de Farmacovigilância, devem dispor, em permanência de um posto de trabalho interconversível de presencial para remoto/digital, devendo para tal, ter à sua disposição as ferramentas eletrónicas ou outras necessárias e adequadas, para o seu exercício profissional e para a prossecução das suas atividades sem interrupção.
- » As atividades inerentes ao Sistema de Farmacovigilância devem ser passíveis de serem realizadas e monitorizadas à distância, e os seus responsáveis capazes de operar em remoto. Para que tal ocorra, o posto de trabalho deverá, no mínimo, ter um dispositivo portátil (do tipo computador, tablet ou outro) com acesso a ponto de rede de internet, e um telemóvel com o mesmo nível de acessos que habitualmente tem no posto de trabalho presencial.
- » Deverá ser instituída a utilização de pelo menos uma caixa de correio eletrónico parti-

lhada, especificamente dedicada à Área de Farmacovigilância, com acessos garantidos e testados para QPPV, QPPV *deputy* e demais colaboradores nomeados.

- » Deverão ser realizados periodicamente simulacros sobre as ferramentas e ligações implementadas para testagem do Sistema de Farmacovigilância em condições de distanciamento, no caso de falha pontual, mas também de falha prolongada, incluindo a possibilidade de um cenário de catástrofe.
- » Deverá ser considerada a transferência de todo o arquivo físico (papel ou outro) para formato digital. A tarefa poderá ser executada gradualmente no tempo, mas com uma cadência ininterrupta, de forma a evitar que qualquer destruição física de formato papel, não possa ser passível de recuperação posteriormente ao evento.
- » Caso exista uma CRO subcontratada como entidade externa à organização, esta deverá também ter um BCP, e conseqüentemente, ter instituído o seu próprio plano de recuperação de dados. Quando for a CRO a entidade que assegure a transmissão eletrónica de reações adversas para as autoridades competentes, deverá ter registos de simulacros que permitam garantir a funcionalidade do sistema de transmissão aos vários organismos, em situações de eventual catástrofe.

As organizações devem garantir que as bases de dados de Farmacovigilância, BDRA e BDIS e arquivo geral de Farmacovigilância, em particular o arquivo digital de farmacovigilância (ADF), são de acesso restrito através de login e *password*, obedecem à proteção de dados dos utilizadores e seguem uma política de execução de cópias/*backups*, implementada a vários níveis, como exemplo:

- » Realização de cópia local 2 x dia para recuperação direta (07:00 e 12:00).
- » Realização de cópia diária para unidade de armazenamento externo (durante a noite).
- » Sincronização das pastas que contêm as bases de dados nos servidores da entidade / organização para uma nuvem corporativa, por exemplo do tipo de *Microsoft Office 365*. Este sistema permite o acesso aos dados 24/h sobre 7 dias a partir de qualquer local. Todos os acessos restritos e permissões deverão ser os mesmos dos servidores internos. Deverá ser mantida a política de proteção de dados individuais para todos os utilizadores, em todas as bases de dados e servidores da organização.

Após uma disrupção de qualquer etiologia, a equipa de STI segue os procedimentos técnicos com vista à reposição da normalidade dos sistemas informáticos no mais curto espaço de tempo possível. Se os servidores estão dentro das instalações, a existir um problema grave que não permita o acesso físico, o mais provável é que também ocorram problemas com as infraestruturas de suporte às comunicações, o que por sua vez impedirá o acesso às caixas de correio eletrónico. Durante esse período, o acesso às bases de dados deverá ser assegurado através do acesso direto a uma nuvem corporativa, por exemplo *Microsoft Office 365*, a partir dos computadores portáteis dos colaboradores e mediante uma ligação à internet. Caso a inacessibilidade ao edifício se prolongue no tempo e a atividade da *Contract Research Organization* (CRO) também esteja comprometida (porque situada na mesma zona de afetação da organização, por um evento de grandes dimensões tal como um terramoto ou outra catástrofe), solicitar o apoio dos recursos humanos e técnicos existentes de filial da CRO em outra zona não afetada. Nas situações em que existe perda ou destruição, parcial ou total, do ADF por anomalias da rede informática, dever-se-á solicitar à

equipa de STI a reposição das cópias de segurança mais recentes disponíveis. Em caso de perda definitiva, parcial ou total, do ADF ao nível do sistema informático da organização (incêndio, terramoto, inundação), o acesso às bases de dados pode ser assegurado através do acesso direto a uma nuvem de informação corporativa do tipo do *Microsoft Office 365* ou outra, a partir dos computadores portáteis dos colaboradores e mediante uma ligação à internet. No caso de destruição física de documentos do arquivo digital de farmacovigilância (AGF), estes na medida do possível deverão estar copiados no arquivo digital, ou seja, deverão ser repostos por via do ADF constituído como backup ao AGF (incluindo documentação em papel).

Em caso de eventual falência da EVWEB na origem/EMA, a organização ou a CRO aplicará o seu próprio procedimento interno para esta situação, respeitando as recomendações standard da EMA conhecidas como *EudraVigilance backup procedures*. Caso existam dificuldades de transmissão via EVWEB por indisponibilidade da CRO, o *Qualified Person for Pharmacovigilance* (QPPV) ou o QPPV *deputy*, coordenará o envio, caso a caso e para as autoridades implicadas, da informação de segurança de notificação imediata obrigatória, nomeadamente relatos de reações adversas, utilizando o modelo CIOMS acompanhado de uma carta de rosto que explicará o contexto da notificação e terá explícito que a mesma ocorrerá novamente via EVWEB logo que a normalidade seja reposta.

Nota: no caso das atividades inerentes à área regulamentar, esta pode tomar como modelo *worst case* o *Business Continuity Plan* (BCP) da farmacovigilância e com as devidas adaptações, aplicá-lo à sua área de atividade.

## F. GLOSSÁRIO E ACRÓNIMOS

**ADF** - Arquivo Digital de Farmacovigilância

**AGF** - Arquivo Geral de Farmacovigilância (incluindo documentos em papel e/ou outro)

**AIM** - Autorização de Introdução no Mercado de um Medicamento

**BCP** - *Business Continuity Plan*

**BDIS** - Base de Dados de Informação de Segurança

**BDRA** - Base de Dados de Reações Adversas

**CIOMS** - Formulário internacional standard de transmissão de reações adversas

**CRO** - *Contract Research Organization* (Organização externa contratada para prestação de serviços e consultadoria na área da Farmacovigilância)

**EMA** - Agência Europeia do Medicamento

**EVWEB** - Ferramenta de transmissão via internet de informação de farmacovigilância da EMA

**GCN** - Gestão da Continuidade do Negócio

**INFARMED** - Autoridade Nacional do Medicamento e Produtos de Saúde, I. P.

**RAM** - Reação Adversa a Medicamentos

**RCM** - Resumo das Características do Medicamento

**PSMF** - *Pharmacovigilance System Master File* (Dossier Principal do Sistema de Farmacovigilância)

**QPPV** - *Qualified Person for Pharmacovigilance* (Pessoa Responsável pelo Sistema de Farmacovigilância)

**QPPV Deputy (QPPV backup)** - Pessoa que substitui o QPPV em caso de impossibilidade de contacto deste e que conhece e tem acesso a todas as ferramentas informáticas para desempenhar o cargo devendo, adicionalmente, ser-lhe disponibilizado o acesso permanente a um médico de preferência com conhecimentos na área da farmacovigilância. O papel da CRO poderá, caso o *deputy* QPPV ache necessário, ser reforçado durante a ausência do QPPV

**Q&A** - *Questions and Answers* (Perguntas e Respostas)

**SDEA** - *Safety Data Exchange Agreement* (Acordo para troca de informação no âmbito da farmacovigilância)

**STI** - Sistemas e Tecnologias de Informação

**TI** - Tecnologia de Informação

## G. REFERÊNCIAS BIBLIOGRÁFICAS

1. Infarmed I.P. [Online] [Citação: 8 de abril de 2021]. <https://www.infarmed.pt/web/infarmed/infarmed>;
2. European Medicines Agency. Brexit Preparedness Business Continuity Plan [Online] [Citação: 8 de abril de 2021];
3. European Medicines Agency. European Medicines Regulatory Network COVID-19 Business Continuity Plan [Online] [Citação: 8 de abril de 2021]; [https://www.ema.europa.eu/en/documents/other/european-medicines-regulatory-network-covid-19-business-continuity-plan\\_en.pdf](https://www.ema.europa.eu/en/documents/other/european-medicines-regulatory-network-covid-19-business-continuity-plan_en.pdf)
4. ISO 22301 – Certificação – Gestão da Continuidade de Negócio [Online] [Citação: 8 de abril de 2021]. <https://www.sgs.pt/pt-pt/public-sector/quality-health-safety-and-environment/sustainability/economic-sustainability/iso-22301-certification-business-continuity-management>;
5. Faculdade de Farmácia da Universidade de Lisboa. COVID-19 | Medidas de Contingência na FFUL. 2022. <https://www.ff.ulisboa.pt/noticias/covid-19-medidas-de-contingencia-na-fful/>.

| VERSÃO              | DATA       | ALTERAÇÕES     |
|---------------------|------------|----------------|
| Nº 70-NGE-01-011-00 | 15.04.2021 | Novo Documento |

Verificado pela Comissão Executiva a 05.07.2023 | Aprovado pela Direção Nacional da OF a 11.07.2023



ORDEM DOS FARMACÊUTICOS 2023