

Relatório do trabalho da disciplina de Cibersegurança

## Plano Segurança 4Pharma

---

António Jorge Magalhães da Rocha - 26052

António Jorge Gonçalves de Sá - 30401

Adelino Daniel da Rocha Vilaça - 16939

António Rafael Ferreira - 26402

Licenciatura em Engenharia de Sistemas Informáticos

Maio de 2025

Afirmo por minha honra que não recebi qualquer apoio não autorizado na realização deste trabalho prático.  
Afirmo igualmente que não copiei qualquer material de livro, artigo, documento web ou de qualquer outra fonte exceto onde a origem estiver expressamente citada.

António Jorge Magalhães da Rocha - 26052

António Jorge Gonçalves de Sá - 30401

Adelino Daniel da Rocha Vilaça - 16939

António Rafael Ferreira - 26402

# Índice

<b>GLOSSÁRIO</b>	<b>VIII</b>
<b>1 SUMÁRIO</b>	<b>9</b>
1.1 Objetivo do Plano	9
1.2 Âmbito	9
1.3 Principais Riscos e Estratégias de Mitigação	10
1.3.1 Risco de Compromisso da Qualidade e Segurança dos Medicamentos	10
1.3.2 Risco de Interrupção e Falhas na Cadeia de Fornecimento	10
1.3.3 Risco de Violiação de Dados e Perda de Propriedade Intelectual	10
1.3.4 Risco de Incumprimento Regulatório	11
<b>2 INTRODUÇÃO</b>	<b>12</b>
2.1 Apresentação	12
2.2 Importância da Segurança no Setor Farmacêutico	12
2.3 Contexto Regulatório	12
<b>3 ESTRUTURA</b>	<b>13</b>
3.1 Governação de Segurança e Framework de Gestão de Risco	13
3.2 Comitê de Segurança da Informação	13
3.2.1 Composição Proposta	13
3.2.2 Responsabilidades	13
3.2.3 Frequência de Reuniões:	14
3.3 Responsabilidades (RACI)	14
3.4 Grupos de trabalho especializados	15
3.4.1 GT1 - Proteção de Propriedade Intelectual	15
3.4.2 GT2 - Conformidade Regulamentar	15
3.4.3 GT3 - Continuidade de Negócio	15
3.5 Frameworks e Metodologias Adotadas	15
3.5.1 Framework Principal: COBIT 2019	15

3.5.2	Domínios Aplicados:	16
3.5.3	Metodologia de Avaliação de Risco: OCTAVE-S	16
3.6	Normas e Standards Complementares	17
3.7	Legislação e Regulamentação Aplicável	17
3.7.1	Regulamentação de Proteção de Dados	17
3.7.2	Regulamentação Farmacêutica Específica	17
3.7.3	Normas de Segurança Específicas	18
3.8	Modelo de Maturidade de Segurança	19
3.8.1	Níveis de maturidade (baseado em CMMI)	19
3.8.2	Roadmap de maturidade	19
3.9	Orçamentos e Recursos	20
3.9.1	Investimento por Área (1º ano)	20
3.9.2	Retorno do Investimento Esperado	20
3.10	Cultura de Segurança	20
3.10.1	Programa de Consciencialização	20
3.10.2	Incentivos e Responsabilização	21
<b>4</b>	<b>PLANO DE SEGURANÇA DA INFORMAÇÃO</b>	<b>22</b>
4.1	Contexto Organizacional	22
4.1.1	Perfil da Organização	22
4.1.2	Ativos críticos de informação	22
4.2	Metodologia Octave	23
4.2.1	Fase 1: Construir Perfis de Ameaças Baseados em Ativos	23
4.2.2	Fase 2: Identificar Vulnerabilidades	24
4.2.3	Fase 3: Desenvolver Estratégia e Planos de Segurança	25
4.3	Análise e Gestão de Riscos	25
4.3.1	Avaliação de Riscos	26
4.3.2	Matriz de Riscos Visual	27
4.4	Controlos de Segurança (Baseados em COBIT)	27

4.4.1	Framework – COBIT -5	27
4.4.2	Controlos de Governação e Gestão	28
4.4.3	Controlos Técnicos Específicos	29
4.4.4	Controlos Organizacionais	30
4.5	Conformidade Regulamentar	31
4.5.1	Requisitos INFARMED/EMA/FDA	31
4.5.2	Requisitos RGPD - Pseudonimização vs Anonimização	32
4.6	Plano de Resposta a Incidentes	34
4.6.1	Classificação de Incidentes	34
4.7	Métricas e KPIs	34
4.7.1	Métricas de Segurança	35
4.7.2	Métricas de Conformidade	36
4.8	Orçamento e Recursos	37
<b>5</b>	<b>CONFORMIDADE COM TRIAL MASTER FILE (TMF) DIGITAL</b>	<b>37</b>
5.1.1	Requisitos EMA para eTMF	38
5.1.2	Segregação de Responsabilidades TMF	38
<b>6</b>	<b>PLANO DE CONTINUIDADE E RECUPERAÇÃO DE DESASTRES</b>	<b>40</b>
6.1.1	RTO/RPO por Sistema	40
6.1.2	Estratégia de Backup para 25+ Anos	40
<b>7</b>	<b>ROADMAP DE IMPLEMENTAÇÃO ATUALIZADO</b>	<b>40</b>
7.1.1	Fase 1: Fundação e Conformidade Urgente (Meses 1-3)	40
7.1.2	Fase 2: Proteção Crítica e Pseudonimização (Meses 4-6)	40
7.1.3	Fase 3: Conformidade Total (Meses 7-9)	41
7.1.4	Fase 4: Maturidade e Melhoria Contínua (Meses 10-12)	41
7.2	Considerações Finais e Alertas Críticos	41
<b>8</b>	<b>PLANO DE PROTEÇÃO</b>	<b>42</b>
8.1	R01 – Roubo de Propriedade Intelectual	42
8.2	R02 – Violiação de Dados de Ensaios Clínicos	43

8.3	R03 – Acesso não autorizado a Dados de Pacientes	44
8.4	R04 – Divulgação de preços diferenciados	44
8.5	R05 – Comprometimento do Processo de Produção (PBF)	45
8.6	R06 – Indisponibilidade do Sistema de Farmacovigilância	46
8.7	R07 – Acesso indevido a fórmulas de genéricos	47
8.8	R08 – Perda de dados de colaboradores	47
8.9	R09 – Falha em auditorias	48
8.10	R10 – Ataque Ransomware	49
<b>9</b>	<b>PLANO DE RECUPERAÇÃO</b>	<b>50</b>
9.1	Objetivo	50
9.2	Âmbito	50
9.3	Estratégia Geral de Recuperação	50
9.4	Fases do Processo de Recuperação	51
9.5	Guia de Recuperação por Recurso	51
9.6	Papéis e Responsabilidades (RACI)	53
9.7	KPIs de Recuperação	53
9.8	Testes e Exercícios	53
9.9	Recursos e Ferramentas	54
9.10	Integração com Contingência e Reposição	54
<b>10</b>	<b>PLANO DE CONTINGÊNCIA</b>	<b>54</b>
10.1	Objetivo	54
10.2	Plano de contingência da 4Pharma	55
10.2.1	R01 – Roubo de Fórmulas Patenteadas	55
10.2.2	R02 – Violação de Dados de Ensaios Clínicos	55
10.2.3	R03 – Acesso Indevido a Dados de Pacientes	56
10.2.4	R04 – Divulgação de Preços Diferenciados	56
10.2.5	R05 – Comprometimento do Processo Fabril (PBF)	57
10.2.6	R06 – Indisponibilidade da Plataforma de Farmacovigilância	57

10.2.7	R07 – Acesso Indevido a Fórmulas Genéricas	58
10.2.8	R08 – Perda de Dados de Colaboradores	58
10.2.9	R09 – Falha em Auditorias	59
10.2.10	R10 – Ataque Ransomware Massivo	59
<b>11</b>	<b>PLANO DE REPOSIÇÃO</b>	<b>60</b>
11.1	Objetivo	60
11.2	Âmbito	60
11.3	Princípios Orientadores	61
11.4	Fases do Processo de Reposição	61
11.5	Procedimentos Específicos por Risco	62
11.6	Guia de Reposição	62
11.7	Papeis e Responsabilidades (RACI)	64
11.8	KPIs de Reposição	64
11.9	Testes e Exercícios	65
11.10	Requisitos de Documentação	65
11.11	Requisitos de Recursos	66
<b>12</b>	<b>PLANO DE AÇÃO IMEDIATA (FIRE-DRILL)</b>	<b>66</b>
12.1	Objetivos	66
12.2	Âmbito	66
12.3	Princípios-Chave	66
12.4	Fluxo de Ação	67
12.5	Estrutura da Equipa de Incidente (Incident Command)	67
12.6	Check-List “Go / No Go” para conter Sistema Afetado	68
12.7	Comunicação - modelos rápidos	68
12.8	Critérios de Encerramento do Fire-Drill	68
12.9	KPIs do Fire-Drill	69
12.10	Integração com os restantes planos	69
12.11	Revisão e Treino	69

13	CONCLUSÃO	70
14	ANEXOS	71
A.	Arquitetura / Flow do sistema e/ou negócio (Explicação) – Imagem via Napkin (Light / Dark)	
	71	

## **Lista de Tabelas**

Tabela 1 - Legenda: R = Responsável, A = Accountable, C = Consultado, I = Informado	14
Tabela 2 - 1 Muito Baixo; 2 - Baixo; 3 - Médio; 4 - Alto; 5 - Crítico	24

## **Lista de Figuras**

Figura 1 - Acesso a fórmulas genéricas	30
Figura 2 - Acesso a fórmulas patenteadas	30

## Glossário

CISO – Chief Information Security Officer

GxP – Good x Practice, quality guidelines and regulations

GMP - Good Manufacturing Practice

DPO - Data Protection Officer

DLP – Data Loss Prevention

SIEM – Security information and event management

BYOD – Bring Your Own Device

PBF – Práticas de Bom Fabrico

GMP – Good Manufacturing practices

RBAC – Role Based Access Control

NDA – Non-Disclosure Agreement

TMF – Trial Master File

ALCOA+ - Atribuível, Legível, Contemporâneo, Original, Exato, "+" (Completo, Consistente, Duradouro, Disponível)

NTP – Network Time Protocol

SLA – Service Level Agreement

Pseudonimização - tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares

AIPD – Avaliação de impacto sobre a proteção de dados

## 1 Sumário

### 1.1 Objetivo do Plano

Este Plano de Segurança tem como finalidade salvaguardar a integridade, confidencialidade e disponibilidade dos ativos críticos da 4Pharma bem como a continuidade das operações no contexto da indústria farmacêutica. Pretende-se estabelecer um conjunto de políticas, procedimentos e controlos para proteger a empresa contra ameaças que possam comprometer a sua capacidade de pesquisar, desenvolver, produzir e distribuir medicamentos e produtos biotecnológicos de forma segura e eficaz. Adicionalmente, o plano almeja assegurar a conformidade com as regulamentações do setor farmacêutico impostas por entidades como o INFARMED, a Agência Europeia de Medicamentos (EMA) e a Administração dos Alimentos e Medicamentos (Food and Drug Administration - FDA), protegendo a segurança dos doentes e mantendo o mote da 4Pharma ao nível do seu compromisso ético, de qualidade e de responsabilidade social.

### 1.2 Âmbito

O presente Plano de Segurança abrange todas as áreas operacionais e processos de negócio da 4Pharma, incluindo:

1. Investigação e Desenvolvimento (I&D): Proteção da propriedade intelectual, dados de pesquisa, ensaios clínicos e informações relacionadas com a conceção de novos fármacos, incluindo o uso de inteligência artificial e modelação computacional.
2. Cadeia de Fornecimento: Gestão de riscos associados ao fornecimento de materiais, incluindo a avaliação de fornecedores e a garantia da qualidade e conformidade dos materiais recebidos.
3. Produção: Segurança dos processos de fabrico, minimização de falhas, garantia da qualidade dos produtos, e cumprimento das Práticas de Bom Fabrico (PBF).
4. Farmacovigilância e Segurança dos Medicamentos: Processos de tratamento de denúncias de qualidade, efeitos secundários inesperados, averiguación interna, comunicação às autoridades e gestão de recolha e resarcimento de produtos.
5. Processo de Encomenda e Distribuição: Segurança da informação de clientes e encomendas, processos de pagamento, e logística de entrega e exportação.
6. Sistemas de Informação e Infraestrutura: Proteção dos sistemas tecnológicos que suportam todas as operações da empresa.

### 1.3 Principais Riscos e Estratégias de Mitigação

O plano de segurança identifica e detalha diversos riscos, destacando-se os seguintes como prioritários os seguintes:

#### 1.3.1 Risco de Compromisso da Qualidade e Segurança dos Medicamentos

Ameaças como contaminação microbiológica ou química, desvios nos parâmetros de fabrico, falhas no controlo de qualidade, ou tratamento inadequado de eventos adversos, podem levar a produtos defeituosos, afetar a segurança do doente e resultar em sanções regulamentares.

Estratégia de Mitigação: Implementação rigorosa e monitorização contínua das Práticas de Bom Fabrico (PBF), processos robustos de controlo de qualidade em todas as fases, e um sistema de farmacovigilância proativo e eficiente, incluindo canais de comunicação 24h para reporte.

#### 1.3.2 Risco de Interrupção e Falhas na Cadeia de Fornecimento

Problemas como qualidade inconsistente de matérias-primas, dependência de fornecedores únicos, incumprimento regulatório por parte de fornecedores, ou falhas logísticas podem-se traduzir num impacto na produção, na disponibilidade de medicamentos e na conformidade.

Estratégia de Mitigação: Avaliação contínua e rigorosa de fornecedores para assegurar conformidade com padrões internacionais, diversificação de fontes de materiais críticos (quando viável), e planeamento logístico detalhado com monitorização.

#### 1.3.3 Risco de Violação de Dados e Perda de Propriedade Intelectual

Acesso não autorizado, roubo ou fuga de informação sensível, como dados de I&D, informações de patentes, dados de pacientes e grupos teste, informações financeiras ou algoritmos de IA, representa uma ameaça significativa à competitividade e reputação da 4Pharma.

Estratégia de Mitigação: Implementação de controlos de acesso robustos, encriptação de dados sensíveis, políticas de segurança da informação, formação de colaboradores e medidas de cibersegurança avançadas para proteger os sistemas e as bases de dados.

#### **1.3.4 Risco de Incumprimento Regulatório**

Falha em cumprir com as normativas do INFARMED, EMA, FDA e outras legislações aplicáveis pode resultar em sanções, interrupção da comercialização, e danos à reputação.

Estratégia de Mitigação: Manutenção de um sistema de gestão da qualidade e conformidade atualizado, realização de auditorias internas e externas regulares, formação contínua dos colaboradores sobre os requisitos regulatórios, e processos claros para a comunicação com as autoridades reguladoras.

## 2 Introdução

### 2.1 Apresentação

A 4Pharma é uma empresa farmacêutica especializada na pesquisa, desenvolvimento, produção e distribuição de medicamentos e de produtos biotecnológicos destinados ao mercado médico e farmacêutico. Com uma vasta gama terapêutica que inclui medicamentos genéricos, produtos com princípios ativos patenteados e terapias inovadoras em fase experimental, a 4Pharma posiciona-se como uma empresa de referência a nível mundial. A sua atividade abrange desde a conceção de novos fármacos, recorrendo a ferramentas como inteligência artificial e modelação computacional, até à sua disponibilização aos pacientes através de entidades parceiras autorizadas ou diretamente.

### 2.2 Importância da Segurança no Setor Farmacêutico

No setor farmacêutico, a segurança é um pilar fundamental que sustenta todas as atividades da empresa. A 4Pharma destaca-se pelo seu firme compromisso com a ética e a segurança em todas as suas operações. A empresa assume a responsabilidade social de implementar as melhores práticas durante as fases de aprovação dos produtos, bem como na sua produção, com o objetivo de assegurar a máxima qualidade e confiança. Esta dedicação não só protege os doentes, mas também contribuiativamente para o avanço e a credibilidade do setor médico e farmacêutico. A gestão rigorosa de riscos em todas as fases da operação, desde a investigação e desenvolvimento até ao fornecimento de materiais e produção, é uma prova deste compromisso.

### 2.3 Contexto Regulatório

A 4Pharma opera num ambiente altamente regulado, atuando em estrita conformidade com as diretrizes e exigências de várias entidades reguladoras de renome. Estas incluem o INFARMED (Autoridade Nacional do Medicamento e Produtos de Saúde, I.P.) em Portugal, a Agência Europeia de Medicamentos (EMA) a nível europeu, e a Food and Drug Administration (FDA) nos Estados Unidos. Estas organizações são responsáveis por estabelecer as normas e fiscalizar a indústria farmacêutica, garantindo a segurança, eficácia e qualidade dos medicamentos disponibilizados à população. A adesão a estas regulamentações é crucial não apenas para a legalidade das operações da 4Pharma, mas também para a manutenção da confiança dos seus clientes e parceiros.

### 3 Estrutura

#### 3.1 Governação de Segurança e Framework de Gestão de Risco

A gestão da segurança na 4Pharma requer uma estrutura de governação clara, com papéis e responsabilidades bem delimitados, e a adoção de frameworks de gestão de risco reconhecidas orientem a identificação, avaliação e tratamento dos riscos de segurança de forma continua.

#### 3.2 Comité de Segurança da Informação

Por forma a assegurar uma abordagem abrangente e integrada à segurança da informação, foi definida um grupo de trabalho multidisciplinar para avaliar a segurança de informação. Este órgão de governação reunirá várias competências, desde técnicas, regulamentação e de negócio, desta forma assegurando que todas as perspetivas sejam consideradas nas decisões de segurança. A componente multidisciplinar deste grupo de trabalho é fundamental no setor farmacêutico, dado que a segurança de informação cruza áreas tão distintas como a investigação, a produção, a conformidade legislativa e a proteção de dados pessoais.

##### 3.2.1 Composição Proposta

###### **Presidente:**

- Chief Information Security Officer (CISO) – a nomear

###### **Membros Permanentes:**

- Diretor de I&D (proteção de propriedade intelectual)
- Diretor de Produção (integridade dos processos GMP)
- Diretor de TI (infraestrutura e sistemas)
- Responsável de Farmacovigilância (segurança 24/7)
- Diretor Jurídico (conformidade regulamentar)
- Data Protection Officer (DPO - requisito RGPD)
- Diretor de Qualidade (sistemas GxP)
- Diretor Financeiro (orçamento e investimentos)

##### 3.2.2 Responsabilidades

- Aprovar políticas e procedimentos de segurança

- Supervisionar a implementação do plano de segurança
- Avaliar e priorizar riscos empresariais
- Alocar recursos para iniciativas de segurança
- Reportar ao Conselho de Administração trimestralmente

### 3.2.3 Frequência de Reuniões:

- Ordinárias: Mensalmente;
- Extraordinárias: Sempre que necessário.

## 3.3 Responsabilidades (RACI)

Para garantir clareza e evitar sobreposições ou lacunas nas responsabilidades de segurança, foi adotado o modelo RACI (Responsible, Accountable, Consulted, Informed). Este modelo define inequivocamente quem executa, quem aprova, quem deve ser consultado e quem deve ser informado em cada processo crítico de segurança.

**Tabela 1 - Legenda: R = Responsável, A = Accountable, C = Consultado, I = Informado**

Atividade	CISO	DPO	Dir I&D	Dir. Prod	Dir. TI	Dir. Qual
Política de Segurança	A/R	C	C	C	C	I
Gestão de Acessos PI	C	I	R	I	A	I
Proteção de Dados Pessoais	C	A/R	I	I	C	I
Conformidade GxP	C	I	C	R	C	A
Resposta a Incidentes	A/R	C	I	I	R	C
Auditórias Internas	A	C	I	I	R	R

### 3.4 Grupos de trabalho especializados

Complementando o Comité de Segurança, foram definidos grupos de trabalho especializados para abordar desafios específicos que requerem conhecimento aprofundado e cuidado mais minucioso, estes grupos reportam diretamente ao Comité de Segurança e são compostos por especialistas das áreas consideradas relevantes, permitindo uma análise detalhada e propostas de solução diferenciadas.

#### 3.4.1 GT1 - Proteção de Propriedade Intelectual

**Foco:** Segurança de fórmulas patenteadas vs genéricas

**Líder:** Diretor de I&D

**Membros:** CISO, Jurídico, Gestores de Produto

#### 3.4.2 GT2 - Conformidade Regulamentar

**Foco:** RGPD, INFARMED, EMA, GMP

**Líder:** DPO

**Membros:** Qualidade, Jurídico, Farmacovigilância

#### 3.4.3 GT3 - Continuidade de Negócio

**Foco:** Disaster Recovery (Recuperação), disponibilidade 24/7

**Líder:** Diretor de TI

**Membros:** Produção, Farmacovigilância, Vendas

### 3.5 Frameworks e Metodologias Adotadas

#### 3.5.1 Framework Principal: COBIT 2019

Framework abrangente que integra governação e gestão de TI, alinhado com os objetivos empresariais da 4Pharma.

### **3.5.2 Domínios Aplicados:**

1. EDM (Evaluate, Direct and Monitor)
  - a. EDM01: Governação
  - b. EDM03: Gestão de Risco
  - c. EDM05: Gestão de Stakeholders
2. APO (Align, Plan and Organize)
  - a. APO01: Framework de Gestão
  - b. APO12: Gestão de Risco
  - c. APO13: Gestão de Segurança
3. DSS (Deliver, Service and Support)
  - a. DSS05: Gestão de Segurança de Serviços
  - b. DSS06: Gestão de Continuidade

### **3.5.3 Metodologia de Avaliação de Risco: OCTAVE-S**

Metodologia específica para organizações de média dimensão, focada em ativos críticos.

1. Fases de Implementação:
  - a. Fase 1: Identificação de ativos críticos e requisitos de segurança
  - b. Fase 2: Identificação de vulnerabilidades da infraestrutura
  - c. Fase 3: Desenvolvimento de estratégias e planos de segurança
2. Aplicação Específica 4Pharma:
  - a. Diferenciação clara entre ativos de alta criticidade (fórmulas patenteadas) e baixa criticidade (genéricos)
  - b. Foco em conformidade regulamentar farmacêutica
  - c. Integração com requisitos de farmacovigilância

### 3.6 Normas e Standards Complementares

Standard	Aplicação	Prioridade
ISO/IEC 27001:2022	Sistema de Gestão de Segurança da Informação	Alta
ISO/IEC 27701:2019	Extensão para gestão de privacidade (RGPD)	Alta
NIST SP 800-14	Princípios gerais de segurança	Média
21 CFR Part 11	Registos eletrónicos e assinaturas (FDA)	Alta
GAMP 5	Validação de sistemas computorizados (GxP)	Alta

### 3.7 Legislação e Regulamentação Aplicável

#### 3.7.1 Regulamentação de Proteção de Dados

RGPD (Regulamento 2016/679)

- Aplicável a todos os dados pessoais (colaboradores, pacientes, parceiros);
- Requisitos especiais para dados de saúde (Art.º 9);
- Obrigações de pseudonimização para ensaios clínicos;
- Nomeação obrigatória de DPO.

Lei Nacional de Proteção de Dados

- Lei n.º 58/2019 (execução do RGPD em Portugal);
- Poderes da CNPD para fiscalização e sanções.

#### 3.7.2 Regulamentação Farmacêutica Específica

EU Clinical Trials Regulation 536/2014

- Retenção de dados de ensaios clínicos: 25 anos;
- Requisitos para Trial Master File (TMF);
- Sistema CTIS obrigatório desde 31/01/2023;
- Transição completa até 31/01/2025.

Diretiva 2001/83/EC (Código Comunitário Medicamentos)

- Farmacovigilância contínua;
- Retenção de dados de segurança: 10 anos;
- Relatórios periódicos de segurança (PSUR);

EudraLex Volume 4 - GMP Guidelines

- Integridade de dados (ALCOA+);
- Validação de sistemas computorizados;
- Audit trails e registos eletrónicos.

Regulamentação INFARMED

- Decreto-Lei n.º 176/2006 (Estatuto do Medicamento);
- Deliberação n.º 105/CA/2007 (Boas Práticas);
- Circular informativa N.º 184/CD/550.20.001.

### 3.7.3 Normas de Segurança Específicas

NIS2 (Diretiva 2022/2555)

- Aplicável ao setor farmacêutico como "entidade essencial";
- Requisitos de cibersegurança reforçados;
- Notificação de incidentes em 24h;
- Em transposição para lei nacional.

ISO 27799:2016

- Segurança da informação em saúde;
- Complementa ISO 27002 para contexto médico.

## 3.8 Modelo de Maturidade de Segurança

### 3.8.1 Níveis de maturidade (baseado em CMMI)

Nível	Descrição	Estado Atual	Meta (12 meses)
1 – Inicial	Processos ad-hoc	Feito	
2 – Gerido	Processos definidos por projeto	Andamento	Objetivo
3 – Definido	Processos organizacionais		Objetivo
4 – Quantitativamente Gerido	Métricas e KPIs		
5 - Otimizado	Melhorias		

### 3.8.2 Roadmap de maturidade

S1 2025: Estabelecer Fundações

- Nomear CISO e completar Comité
- Aprovar políticas base
- Implementar OCTAVE-S Fase 1

S2 2025: Implementar Controlos

- Deploy de soluções técnicas prioritárias
- Validar processos GxP
- Iniciar certificação ISO 27001

S1 2026: Conformidade Total

- Auditoria RGPD completa
- Conformidade CTR verificada
- Testes de disaster recovery

S2 2026: Otimização

- Métricas e dashboards implementados
- Processos de melhoria contínua
- Preparação para NIS2

## 3.9 Orçamentos e Recursos

### 3.9.1 Investimento por Área (1º ano)

Área	Descrição	Orçamento
Pessoal	CISO, DPO, 2 analistas	300.000
Tecnologia	DLP, SIEM, Encriptação, MFA	250.000
Consultoria	ISSO 270001, OCTAVE -S	100.000
Formação	Awareness, especializada	50.000
Auditórias	Internas e certificação	100.000
Contingência	10%	80.000
Total		880.000

### 3.9.2 Retorno do Investimento Esperado

- Redução de risco de multas RGPD: Até 4% faturação anual
- Proteção de PI: Valor de 1 fórmula patenteada valor superior a €10M
- Continuidade de negócio: Evitar perdas de €100k/dia
- Vantagem competitiva: Certificações como elemento diferenciador

## 3.10 Cultura de Segurança

### 3.10.1 Programa de Consciencialização

Público Geral (todos colaboradores)

- Formação inicial obrigatória (4h)
- Refreshers trimestrais (1h)
- Simulações de phishing mensais
- Newsletter de segurança mensal

Formação Específica por Função

- I&D: Proteção de PI, classificação de dados (8h/ano)
- Clínicos: RGPD, pseudonimização (6h/ano)
- Produção: Integridade de dados, ALCOA+ (6h/ano)
- Vendas: Confidencialidade comercial (4h/ano)

### 3.10.2 Incentivos e Responsabilização

- Inclusão de objetivos de segurança nas avaliações de desempenho
- Reconhecimento trimestral de boas práticas
- Processo disciplinar claro para violações
- Canal de denúncia anônimo para questões de segurança

## 4 Plano de Segurança da Informação

Este plano de segurança foi desenvolvido para a empresa farmacêutica 4Pharma, seguindo uma abordagem baseada em risco, a estrutura do plano reflete a progressão desde a identificação dos ativos críticos até a implementação de controlos específicos, tendo sempre em consideração o contexto regulamentar da indústria farmacêutica.

O plano começa pela análise do contexto operacional, passa pela avaliação de riscos a qual foi baseada na metodologia OCTAVE-S, e termina em controlos e planos de ação concretos, esta abordagem assegura que os aspectos críticos são abordados de forma comprehensível.

### 4.1 Contexto Organizacional

Esta secção descreve a 4Pharma e o ambiente em que opera, fundamental para compreender os requisitos e o âmbito do presente Plano de Segurança.

#### 4.1.1 Perfil da Organização

A 4Pharma caracteriza-se pelos seguintes elementos:

**Nome:** 4Pharma;

**Setor de atividade:** Farmacêutico;

**Principais atividades:** Pesquisa, desenvolvimento, produção e distribuição de medicamentos e de produtos biotecnológicos para o mercado médico e farmacêutico.

**Regulamentação aplicável (principais):**

- INFARMED (Autoridade Nacional do Medicamento e Produtos de Saúde, I.P.)
- EMA (Agência Europeia de Medicamentos)
- FDA (Food and Drug Administration)
- RGPD (Regulamento Geral sobre a Proteção de Dados)

#### 4.1.2 Ativos críticos de informação

A proteção dos ativos de informação é fundamental para o sucesso da 4Pharma, não apenas do ponto de vista comercial, mas também para garantir a segurança dos pacientes e o cumprimento das obrigações regulamentares. A empresa gera diversos tipos de informação crítica, desde

propriedade intelectual resultado de anos de investigação e investimento até dados sensíveis de pacientes em ensaios clínicos.

É importante distinguir entre diferentes níveis de criticidade, por exemplo, enquanto as fórmulas patenteadas representam o núcleo da inovação e vantagem competitiva da empresa, as fórmulas de genéricos, embora importantes, permitem uma abordagem de segurança mais ágil para facilitar a eficiência operacional. Esta diferenciação permite-nos aplicar recursos de forma proporcional ao risco.

A seguinte tabela resume os principais ativos de informação e a sua criticidade:

Categoría	Ativo	Criticidade
Propriedade Intelectual	Fórmulas de medicamentos patenteadas	Critico
Propriedade intelectual	Fórmulas medicamentos genéricos	Média
Dados Clínicos	Dados de ensaios clínicos	Critico
Dados Pessoais	Dados de pacientes (ensaios)	Critico
Dados Comerciais	Preços diferenciados por cliente	Alto
Dados Comerciais	Contratos com hospitais / armazéns	Alto
Dados Operacionais	Processo de produção (PBF)	Alto
Dados de Farmacovigilância	Relatórios de efeitos adversos	Critico

## 4.2 Metodologia Octave

A escolha da metodologia OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small organizations) foi definida como metodologia a ser utilizada avaliação de risco dado que os princípios em que se baseia enquadram-se com a 4Pharma nomeadamente: desenhada para organizações de média dimensão; foca-se em ativos críticos, alinhando-se com nossa necessidade de proteger propriedade intelectual; permite flexibilidade na implementação, adaptando-se ao contexto farmacêutico; Promove que seja envolvida toda a organização, não apenas da equipa técnica

### 4.2.1 Fase 1: Construir Perfis de Ameaças Baseados em Ativos

Nesta fase inicial, trabalhou-se com as diferentes áreas da empresa para identificar: Quais são os ativos verdadeiramente críticos para cada departamento; que tipo de ameaças mais inquietam cada área; qual o impacto real de diferentes cenários de segurança.

Esta abordagem colaborativa garante que o plano de segurança reflita as necessidades do negócio, não apenas preocupações técnicas.

### *Avaliação de Impacto por Ativo*

Ativo	Confidencialidade	Integridade	Disponibilidade
Fórmulas patenteadas	5	5	3
Fórmulas genéricas	3	4	2
Dados ensaios clínicos	5	5	4
Dados pacientes	5	5	3
Dados colaboradores	4	4	2
Preções diferenciados	4	3	2
Processos produção	3	5	4
Dados farmacovigilância	4	5	5

Tabela 2 - 1 Muito Baixo; 2 - Baixo; 3 - Médio; 4 - Alto; 5 - Crítico

#### **4.2.2 Fase 2: Identificar Vulnerabilidades**

A segunda fase da metodologia OCTAVE foca-se em compreender onde se está vulnerável, que pode ser dividido em vulnerabilidades do tipo técnico ou do tipo organizacional, em detalhe:

#### *Vulnerabilidades Técnicas*

Área	Vulnerabilidade	Severidade
Rede	Segmentação inadequada entre I&D e produção	Alta
Acesso	Falta de autenticação multifactor especialmente em sistemas críticos	Alta
Dados	Encriptação inconsistente de dados em repouso	Média
Aplicações	Sistemas legados sem patches de segurança	Alta
Cloud	Configurações incorretas em serviços cloud	Média
Endpoints	Dispositivos móveis não geridos (BYOD)	Média

Desde a falta de segmentação adequada entre as redes de I&D e produção, até à ausência de autenticação multifactor em sistemas críticos. Cada vulnerabilidade é avaliada no contexto do seu potencial impacto nos ativos identificados na Fase 1.

#### *Vulnerabilidade Organizacionais*

Área	Vulnerabilidade	Severidade
Pessoas	Falta de formação em segurança para investigadores	Alta
Processos	Gestão de acessos ad-hoc para dados genéricos	Média
Políticas	Ausência de política clara de classificação de dados	Alta

Terceiros	Controlo inadequado sobre fornecedores	Média
-----------	----------------------------------------	-------

Os maiores riscos, muitas vezes não são técnicos, mas organizacionais, falta de formação adequada, processos informais, ou simplesmente a ausência de políticas claras. A metodologia OCTAVE-S reconhece esta realidade e aborda-a diretamente.

#### 4.2.3 Fase 3: Desenvolver Estratégia e Planos de Segurança

Com base nas duas fases anteriores, desenvolveu-se estratégias de segurança que devem ser proporcionais ao risco identificado, consideram de igual forma soluções técnicas como organizacionais, respeitam as necessidades operacionais da empresa, são economicamente viáveis e sustentáveis.

As estratégias e planos específicos resultantes desta fase são detalhados nas secções seguintes deste documento.

### 4.3 Análise e Gestão de Riscos

A avaliação de riscos na 4Pharma segue uma abordagem que considera tanto a probabilidade de ocorrência como o impacto potencial. Esta análise a duas dimensões permite dar prioridade aos recursos e esforços onde se entende haver maior necessidade.

Cada risco identificado é analisado considerando:

- O contexto específico do setor farmacêutico;
- Os requisitos regulamentares aplicáveis;
- O impacto potencial na segurança dos pacientes;
- As implicações financeiras e danos à reputação, que implicam quebra de confiança.

Os principais riscos identificados na atividade desenvolvida pela 4Pharma são:

- Roubo de Propriedade Intelectual: O risco de potencial roubo de fórmulas patenteadas. Uma única fórmula pode representar anos de investigação e investimentos superiores a 10 milhões de euros. A perda desta informação não apenas prejudicaria a 4Pharma financeiramente, mas poderia comprometer a segurança dos pacientes se a fórmula fosse produzida sem os controlos de qualidade adequados.

- Violação de Dados Pessoais: Com o RGPD em vigor, a violação de dados pessoais quer sejam de pacientes em ensaios clínicos quer sejam de colaboradores, representa não apenas um risco financeiro significativo (multas até 4% da faturação anual), mas também um grave dano reputacional. A confiança é fundamental no setor farmacêutico, e uma violação pode ter consequências duradouras.

- Comprometimento da Integridade de Dados: No contexto em que a empresa desenvolve atividade a integridade dos dados é crítica, alterações não autorizadas em dados de produção ou ensaios clínicos podem ter consequências graves para a segurança dos pacientes e resultar em sanções regulamentares.

Para cada risco definiu-se uma estratégia de tratamento, estas estratégias podem ser:

Mitigar: Para riscos críticos e altos, implementamos controlos para reduzir probabilidade ou impacto;

Aceitar: Para alguns riscos de baixo impacto, especialmente onde a mitigação comprometeria a eficiência operacional;

Transferir: Através de seguros ou acordos contratuais, para riscos específicos;

Para fórmulas genéricas aceitou-se um nível ligeiramente superior de risco (controlos de acesso mais simples) para facilitar a produção eficiente, acrescentando medidas como monitorização reforçada.

#### 4.3.1 Avaliação de Riscos

ID	Risco	Ativo afetado	Probabilidade	Impacto	Nível de risco	Estratégia
R01	Roubo de propriedade intelectual (fórmula patenteadas)	Fórmulas patenteadas	3	5	15	Mitigar
R02	Violação de dados de ensaios clínicos	Dados ensaios	2	5	10	Mitigar
R03	Acesso não autorizado a dados de pacientes	Dados pacientes	3	5	15	Mitigar
R04	Divulgação de preços diferenciados	Preços	4	3	12	Mitigar
R05	Comprometimento do processo de produção (PBF)	Processos Produção	2	5	10	Mitigar
R06	Indisponibilidade do sistema de farmacovigilância	Sistema 24h	2	5	10	Mitigar
R07	Acesso indevido a fórmulas de genéricos	Fórmulas genéricas	4	2	8	Aceitar
R08	Perda de dados de colaboradores	Dados RH	2	3	6	Transferir
R09	Falha em auditorias	Conformidade	2	4	8	Mitigar

R10	Ataque Ransomware	Todos	3	5	15	Mitigar
-----	-------------------	-------	---	---	----	---------

R07 – é aceite o risco para agilizar o processo de produção.

#### 4.3.2 Matriz de Riscos Visual

Impacto		Muito baixa	Baixa	Média	Alto	Muito alto	
Probabilidade	Muito alta						
	Alta						
	Média					R01 / R03 / R10	
	Baixa				R08	R09	R02 / R05 / R06
	Muito baixa						

### 4.4 Controlos de Segurança (Baseados em COBIT)

#### 4.4.1 Framework – COBIT -5

Para garantir uma implementação estruturada e alinhada com as melhores práticas internacionais, a 4Pharma adotou a framework COBIT 5 como base para os seus controlos de segurança. O COBIT 5 foi escolhido por oferecer uma abordagem holística que integra governação e gestão de TI, sendo particularmente adequado para organizações que necessitam demonstrar conformidade regulamentar.

A framework baseia-se em 5 princípios fundamentais:

1. Satisfazer as necessidades das partes interessadas;
2. Cobrir a organização de ponta a ponta;

3. Aplicar um framework único e integrado;
4. Permitir uma abordagem holística;
5. Separar governação de gestão.

#### **4.4.2 Controlos de Governação e Gestão**

O COBIT 5 organiza 37 processos em 5 domínios, para o âmbito da 4Pharma, focou-se os mais relevantes para a segurança da informação.

#### *APO (Align, Plan and Organize) - Alinhar, Planejar e Organizar*

##### APO01 – Gestão da Framework de TI

- Estabelecer o comité (grupo de trabalho) de segurança de informação.
- Definir RACI para segurança de dados farmacêuticos.
- Integrar segurança no processo de desenvolvimento de medicamentos.

##### APO12 – Gestão de Risco

- Implementar processo formal de gestão de risco.
- Realizar avaliações trimestrais de risco.
- Manter registo de riscos atualizado.

#### *DSS(Deliver, Service and Support) – Entregar, Serviço e Suporte*

##### DSS05 - Gerir Serviços de Segurança

- Proteger contra malware.
- Gerir segurança de rede e ligação.
- Gerir segurança de endpoints.
- Gerir identidade e acessos.
- Gerir segurança física.

Adotou-se uma abordagem baseada em risco para a implementação do COBIT 5, selecionando inicialmente os processos mais críticos para o contexto farmacêutico. Esta implementação por fases

focou-se em três processos fundamentais: APO01 (governação), APO12 (gestão de risco) e DSS05 (segurança).

Esta abordagem permite demonstrar resultados rápidos e criar as fundações para uma eventual expansão para outros processos da framework conforme a maturidade organizacional evoluí.

#### 4.4.3 Controlos Técnicos Específicos

Os controlos técnicos foram desenhados considerando as especificidades do setor farmacêutico e os diferentes níveis de criticidade dos ativos.

##### *Proteção de Propriedade Intelectual*

A propriedade intelectual representa o core business da 4Pharma. Os controlos implementados refletem esta criticidade:

Controlo	Descrição	Prioridade
Segmentação da rede	Separar identidade de dados clínicos	Crítica
DLP (Data Loss Prevention)	Monitorizar e bloquear exfiltração de fórmulas	Crítica
Encriptação	AES – 256 para todas as fórmulas	Crítica
Gestão de acessos	RBAC com princípio do menor privilégio	Alta
Auditoria	Logs de todos os acessos a fórmulas	Alta

##### *Proteção de Dados Clínicos e Pessoais (RGPD)*

A conformidade com o RGPD é obrigatória e requer controlos específicos para dados de saúde:

Controlo	Descrição	Prioridade
Pseudonimização	Separar a identidade de dados clínicos	Crítica
Consentimento	Sistema de gestão de consentimentos	Crítica
Direito dos titulares	Portal para exercício de direitos RGPD	Alta
Privacy by design	Integrar privacidade no desenvolvimento	Alta
DPO	Nomear encarregado de Proteção de Dados	Crítica

##### *Controlos Diferenciados por Fórmula*

Reconhecendo a diferença de valor entre fórmulas patenteadas e genéricas, implementou-se uma abordagem de segurança diferenciada:

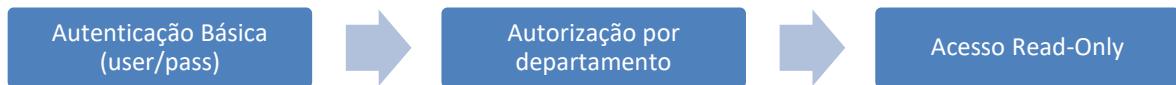


Figura 1 - Acesso a fórmulas genéricas



Figura 2 - Acesso a fórmulas patenteadas

Esta diferenciação permite à 4Pharma manter agilidade na produção de genéricos enquanto assegura proteção máxima para ativos críticos.

#### 4.4.4 Controlos Organizacionais

A componente humana é frequentemente o elo mais fraco na segurança. Por isso, os controlos organizacionais são fundamentais.

##### *Formação e Consciencialização*

O programa foi desenhado para diferentes audiências com conteúdos específicos:

Público-alvo	Conteúdo	Frequência
Investigadores	Proteção de PI, classificação de dados	Trimestral
Equipa de ensaios clínicos	RGPD, confidencialidade médica	Semestral
Vendas	Proteção de informação comercial	Anual
Todos	Phishing, engenharia social	Trimestral

##### *Gestão de Terceiros*

Num setor onde a colaboração com parceiros externos é essencial, a gestão de terceiros assume particular relevância:

- Due diligence (investigação e análise prévia) de segurança para todos os fornecedores críticos;
- Cláusulas contratuais específicas de segurança e confidencialidade;
- Auditorias anuais a fornecedores de serviços críticos;
- Acordos de Confidencialidade (NDAs) reforçados para qualquer acesso a fórmulas ou dados sensíveis.

- Segregação de acessos com princípio need-to-know.

## 4.5 Conformidade Regulamentar

A 4Pharma opera num ambiente altamente regulado, onde o incumprimento pode resultar não apenas em sanções financeiras, mas também na perda de autorização para continuar a sua atividade. A conformidade regulamentar é, portanto, não apenas uma questão legal mas uma questão de sobrevivência empresarial.

### 4.5.1 Requisitos INFARMED/EMA/FDA

Um dos desafios mais significativos no setor farmacêutico é a obrigação de manter dados durante longos períodos longos. O Clinical Trials Regulation (CTR) 536/2014 estabeleceu novos padrões que todas as empresas farmacêuticas devem cumprir, estes períodos de retenção refletem a necessidade de garantir rastreabilidade a longo prazo para proteger a segurança dos pacientes.

#### *Requisitos de Retenção de Dados (CTR 536/2014)*

Tipos de dados	Período Mínimo	Base Legal	Notas
Ensaios Clínicos (TMF)	25 anos	EU CTR 536/2014 art.º 58	Após término do estudo
Medicamentos de Terapia Avançada (ATMPs)	30 anos	Regulamento CE 1394/2007 Art.º 15	Produtos de terapia genética/celular
Dados Farmacovigilância	10 anos	Regulamento EU 520/2012 Art.º 12	Após expirar a autorização
Dados de Produção (GMP)	5 anos	EudraLex Vol. 4, art.º 11	Ou 1 ano após a data de expiração do lote

É essencial entender que esta retenção não significa simplesmente arquivar dados, os dados devem permanecer acessíveis, íntegros e interpretáveis durante todo o período, o que representa um desafio técnico considerável face à evolução tecnológica.

#### *Requisitos de Integridade de Dados*

A integridade de dados no setor farmacêutico vai muito além da simples prevenção de perda de dados. Os princípios ALCOA+ (Attributable, Legible, Contemporaneous, Original, Accurate, plus

Complete, Consistent, Enduring, Available) são um dos padrões aceites por praticamente todas as entidades reguladoras. Cada princípio tem implicações práticas específicas:

ALCOA+	Controlo Implementado	Evidência
Attributable	ID de utilizador único, sem contas partilhadas	Logs de autenticação
Legible	Dados em formato legível durante todo o tempo de retenção	Testes de recuperação
Contemporaneous	Time stamps automáticos, sincronização NTP	Audit trails (caminho de auditoria)
Original	Preservação de dados raw (cru), proibição de transcrições	Políticas de Backup
Accurate	Validações de entradas, checksums	Relatórios de validação
+ Complete	Metadados preservados, contexto mantido	Documentação completa
+ Consistent	Sequência cronológica (evitar gaps)	Análise de logs
+ Enduring	Migrações planeadas, formato não proprietário	Plano de preservação
+ Available	Recuperação em menos de 24h para inspeções	SLAs documentados

O incumprimento destes princípios pode resultar em warning letters da FDA, não-conformidades graves (major) em inspeções EMA, ou mesmo suspensão de autorizações de comercialização.

#### 4.5.2 Requisitos RGPD - Pseudonimização vs Anonimização

##### *Distinção para ensaios clínicos*

Um dos aspetos essenciais de distinguir do RGPD no contexto de ensaios clínicos é a diferença entre pseudonimização e anonimização. Esta distinção não é meramente académica dado que tem implicações práticas profundas para como os dados devem ser geridos:

Técnica	Definição	Status RGPD	Uso recomendado
Pseudonimização	Substituição de identificadores por códigos, reversível com chave	Dados pessoais (âmbito do RGPD)	Ensaio clínico longitudinal
Anonimização	Remoção irreversível de todos os identificadores	Fora do âmbito RGPD	Publicação de resultados

É crucial que todas as equipas compreendam que os dados pseudonimizados continuam a ser dados pessoais aos olhos do RGPD, e como tal requerem todas as proteções associadas.

##### *Implementação de Pseudonimização*

O processo de pseudonimização implementado pela 4Pharma segue as práticas internacionais, garantindo proteção enquanto mantém a utilidade dos dados para investigação:



Para ilustrar com um exemplo prático: imagine-se um paciente, João Pereira, data de nascimento 01/01/1980. No processo de pseudonimização: A chave de correspondência é mantida exclusivamente pelo Site TMF (hospital/centro de investigação); Os dados clínicos são remetidos ao Sponsor TMF (4Pharma) apenas com o código único (ex: PT-C2-2025-001); O Sponsor nunca tem acesso aos identificadores diretos; O processo é protegido com encriptação AES-256; O acesso à chave é rigorosamente segregado e auditado

Esta segregação é fundamental não apenas para conformidade RGPD, mas também para manter a integridade científica do estudo, evitando desta forma viés.

### *Avaliação de Risco de Reidentificação*

Mesmo com pseudonimização adequada, existe sempre algum risco residual de reidentificação, especialmente quando várias fontes de dados podem ser correlacionadas. A solução para a 4Pharma passa uma abordagem que permite avaliar e mitigar estes riscos:

Fator de Risco	Mitigação	Responsável
Dados Raros (doenças raras)	Agregação geográfica, supressão	DPO + Estatístico
Múltiplas fontes	Minimização de dados recolhidos	Investigador principal
Quasi-identificadores	Generalização (idade para faixa etária)	Data Manager
Inferência estatística	k-anonymity, l-diversity	Estatístico

Por "múltiplas fontes" entende-se o risco de cruzamento de dados de diferentes origens (redes sociais, registos públicos, outras bases de dados) que possam levar à re-identificação. A mitigação passa por recolher apenas o mínimo necessário para os objetivos científicos do estudo.

### *Requisitos Específicos por Artigo RGPD*

O RGPD contém vários artigos com implicações diretas para ensaios clínicos. A tabela seguinte elenca os requisitos principais e sua implementação:

Artigo	Requisito	Implementação
--------	-----------	---------------

Art.º 25	Proteção de dados desde a conceção (privacy by design)	Checklist obrigatório em todos os protocolos
Art.º 32	Segurança do tratamento	Encriptação e também Pseudonimização obrigatórias
Art.º 33/34	Notificação de violações	72h à CNPD e também pacientes se risco elevado
Art.º 35	AIPD	Obrigatória para todos os ensaios clínicos
Art.º 89	Salvaguardas para casos de investigação	Pseudonimização e acordos celebrados

É importante notar que o Art.º 89 oferece algumas flexibilidades para investigação científica, mas estas vêm acompanhadas de salvaguardas que devem ser implementadas e documentadas.

## 4.6 Plano de Resposta a Incidentes

### 4.6.1 Classificação de Incidentes

Nível	Descrição	Tempo de resposta máximo	Responsáveis
Critico	Comprometimento de fórmulas patenteadas, violação de dados de pacientes	1 hora	CEO, CISO, DPO
Alto	Indisponibilidade de farmacovigilância, falha em ensaio clínico	2 horas	CISO, diretor da área
Médio	Tentativa de phishing, malware contido	4 horas	Equipa segurança
Baixo	Vulnerabilidade identificada, sem ser explorada	24 horas	Equipa segurança

## 4.7 Métricas e KPIs

A definição e monitorização de métricas é fundamental para avaliar a eficácia implementar melhoria contínua da segurança. Devem ser definidas de forma clara, facilmente mensurável e alinhadas com os objetivos fundamentais e estratégicos da organização.

Permitem avaliar, de forma objetiva, se os controlos técnicos, organizacionais e procedimentais estão a cumprir os objetivos definidos no plano de segurança, bem como identificar desvios, fragilidades ou oportunidades de melhoria.

O acompanhamento e compreensão dos resultados e do seu contexto permite simultaneamente suportar a tomada informada de decisões e demonstrar compromisso com a segurança e a conformidade perante partes interessadas (como, por exemplo, auditores, clientes e entidades reguladoras).

As métricas são aqui agrupadas em duas grandes categorias:

- Métricas de Segurança, que visam medir a eficácia real dos controlos e práticas de proteção da informação.
- Métricas de Conformidade, que avaliam o grau de alinhamento com normas, políticas internas, requisitos legais e contratuais.

A distinção entre ambas é essencial: uma organização pode estar em conformidade sem estar efetivamente segura, e vice-versa. Assim, a combinação das duas perspetivas permite uma visão holística e equilibrada do estado da segurança.

#### 4.7.1 Métricas de Segurança

Avaliam o desempenho real das políticas de segurança — se os sistemas, processos e pessoas estão suficiente e corretamente protegidos, de forma que permita proteger eficazmente a organização contra ameaças.

Estas métricas têm por objetivo avaliar e melhorar a eficácia operacional da segurança, reduzindo o risco de incidentes, perdas de dados ou acessos indevidos. Não têm por objetivo avaliar, garantir ou demonstrar conformidade.

Tipo de métrica	Métrica	Valor Alvo
Controlo de Acessos	Percentagem de contas com privilégios administrativos.	<3%
	Tempo médio de cancelamento de acessos após saída de colaboradores.	<36 horas
	Percentagem de utilizadores com MFA.	>95%
Proteção de sistemas	Percentagem de dispositivos atualizados.	>98%
	Média de tempo até os patches de segurança serem aplicados.	<8 dias
Monitorização e Detecção	Tempo médio de deteção de incidentes (MTTD – Mean Time to Detect).	<12 horas
	Taxa de falsos positivos dos sistemas de deteção.	<10%

Resposta a incidentes	Tempo médio de resposta a incidentes (MTTR – Mean Time to Respond).	<4 horas
	Número de incidentes resolvidos dentro do SLA (Service Level Agreement).	>97%
	Número de exercícios de simulação de resposta realizados.	>3/ano
	Número de incidentes classificados como críticos.	<2/ano
Sensibilização e Formação	Percentagem de colaboradores com formação em cibersegurança.	>95%
	Taxa de não exposição em testes de phishing internos.	>85%
	Taxa de report em testes de phishing internos.	>15%
Conformidade e Auditoria	Percentagem de planos auditados anualmente.	100%
	Tempo médio para corrigir não conformidades.	<20 dias
	Percentagem de sistemas cobertos por avaliações de risco.	>98%
Backup e Recuperação	Percentagem de sucesso de recuperação de backups.	100%
	Tempo médio de recuperação.	<3 dias
	Percentagem de dados cobertos por backups automáticos.	>90%
	Percentagem de dados críticos cobertos por backups automáticos.	100%

#### 4.7.2 Métricas de Conformidade

Avaliam o grau de alinhamento com políticas internas, leis, regulamentos e normas externas (como RGPD, ISO 27001, NIST, etc.). Permitem demonstrar e/ou evidenciar que a organização cumpre as obrigações legais, normativas e contratuais.

De salientar que conformidade não garante necessariamente segurança eficaz.

Tipo de métrica	Métrica	Valor Alvo
Políticas e Documentação	Percentagem de requisitos legais identificados e documentados.	100%
Sistemas e Avaliações Técnicas	Percentagem de sistemas com avaliação de risco realizada.	>95%
	Percentagem de ativos com análise de risco atualizada.	>95%
Auditorias e Não Conformidades	Auditorias FDA/EMA sem findings críticos.	100%
	Percentagem de não conformidades corrigidas dentro do prazo acordado.	>90%
	Tempo médio para corrigir não conformidades identificadas.	20 dias
	Percentagem de departamentos auditados anualmente.	100%

Conformidade Legal e Contratual	Disponibilidade sistema farmacovigilância	>99.9%
	Média de não conformidades por contrato com clientes/fornecedores.	0
	Percentagem de contractos de fornecedores com cláusulas de segurança e proteção de dados.	>95%
	Percentagem de contractos de clientes com cláusulas de segurança e proteção de dados.	>95%
	Número de não conformidades para com a Lei e regulamentos nacionais e internacionais.	0
Recursos Humanos	Percentagem de colaboradores com compromisso de confidencialidade assinado.	100%
	Número de fugas de informação intencionais identificadas, por parte dos colaboradores.	0

## 4.8 Orçamento e Recursos

Investimento estimado (1 ano)

Área	Descrição	Orçamento
Pessoal	CISO, DPO, 2 analistas	300.000
Tecnologia	DLP, SIEM, Encriptação, MFA	250.000
Formação	Programas de consciencialização	50.000
Auditórias	Certificações e auditórias	100.000
Contingência	Resposta a incidentes	80.000
Total		780.000

## 5 Conformidade com Trial Master File (TMF) Digital

O Trial Master File representa a história completa de um ensaio clínico e é um dos elementos críticos durante inspeções. A transição para formatos digitais (eTMF) traz consigo benefícios, mas também novos desafios de conformidade que devem ser cuidadosamente geridos.

### 5.1.1 Requisitos EMA para eTMF

A European Medicines Agency (EMA) publicou orientações específicas para eTMF que vão além da digitalização de documentos, um eTMF conforme não é apenas um repositório eletrónico tem de ser um sistema validado que garanta a integridade, autenticidade e acessibilidade dos documentos essenciais durante todo o ciclo de vida do ensaio e pelos 25 anos subsequentes.

Componente	Requisito	Implementação
Validação	Sistema validado para GxP	Protocolo IQ/OQ/PQ
Audit trail	Completo e inalterável	21 CFR Part 11 compliance
Metadados	Preservados e pesquisáveis	XML/estruturado
Migração	Verificada e documentada	Checksums + validação
Acesso	Disponível durante inspeções	Portal seguro 24/7

Cada componente tem implicações práticas importantes:

- Validação IQ/OQ/PQ: Installation Qualification, Operational Qualification e Performance Qualification garantem que o sistema funciona conforme especificado.
- Audit trail: Deve registrar quem fez o quê, quando e porquê, sem possibilidade de alteração.
- Metadados: Tão importantes quanto os próprios documentos, incluindo contexto e relacionamentos.
- Migração: Quando sistemas são atualizados, a integridade dos dados deve ser mantida de forma demonstrável.
- Acesso 24/7: Inspetores podem solicitar documentos a qualquer momento, exigindo disponibilidade contínua.

### 5.1.2 Segregação de Responsabilidades TMF

Um dos aspectos mais críticos do TMF é a clara segregação entre o que pertence ao Sponsor e o que deve permanecer no Site (quem conduz os ensaios). Esta segregação não é apenas por questões de boas práticas, é essencial para manter a integridade do ensaio e proteger a privacidade dos participantes.

TMF Master	
Sponsor (4Pharma)	Site TMF
Protocolo	Consentimentos
IB (Brochura do Investigador)	Dados fonte

Contratos	Dados ID participantes
Análises estatísticas	Laboratório Local

Esta divisão reflete princípios fundamentais:

No Sponsor TMF (4Pharma) encontram-se:

- Protocolo: O plano guia do estudo, incluindo todas as versões e adendas;
- IB: Toda a informação científica sobre o medicamento experimental;
- Contratos: Acordos com sites (locais de ensaios), CROs (Contract Research Organization), fornecedores;
- Análises estatísticas: Dados agregados de todos os sites, sem identificadores.

No Site TMF permanecem:

- Consentimentos: Documentos assinados pelos participantes, prova do consentimento informado;
- Dados fonte: Registos médicos originais, resultados de exames;
- Identificação: A chave que liga códigos do estudo a participantes reais;
- Laboratório local: Resultados específicos do site antes da codificação.

Esta separação (segregação) garante que:

1. O Sponsor nunca tem acesso direto a informação identificável dos participantes.
2. O Site mantém controlo sobre os dados médicos dos seus pacientes.
3. A integridade científica é mantida através da separação de responsabilidades.
4. Auditorias e inspeções podem verificar conformidade sem comprometer privacidade.

É crucial que todos os colaboradores envolvidos em ensaios clínicos compreendam estas fronteiras e as respeitem rigorosamente, violações a esta separação de responsabilidades (segregação) podem resultar em não-conformidades graves durante inspeções e comprometer a validade do ensaio.

## 6 Plano de Continuidade e Recuperação de Desastres

### 6.1.1 RTO/RPO por Sistema

Sistema	RTO	RPO	Justificação
Farmacovigilância 24h	2 horas	15 min	Segurança do paciente
Dados ensaios clínicos	4 horas	1 hora	Continuidade dos estudos
Fórmulas patenteadas	8 horas	1 hora	Backup encriptado offline
Sistema de vendas	24 horas	4 horas	Impacto comercial médio

### 6.1.2 Estratégia de Backup para 25+ Anos

Fase	Acção	Tecnologia
0-2 anos	Backup online + nearline	SAN e Cloud híbrida
2-10 anos	Arquivo ativo	Object storage e WORM
10-25 anos	Preservação digital	Formato aberto e migração planeada
Verificação	Testes anuais de recuperação	Recuperação parcial documentado

## 7 Roadmap de Implementação Atualizado

### 7.1.1 Fase 1: Fundação e Conformidade Urgente (Meses 1-3)

- Nomear CISO e DPO (Semana 1)
- Implementar retenção 25 anos para TMF (CTR 536/2014)
- Classificar ativos + definir ALCOA+ para cada sistema
- Segregar dados patenteados vs genéricos
- Iniciar programa de formação RGPD + GxP

### 7.1.2 Fase 2: Proteção Crítica e Pseudonimização (Meses 4-6)

- Implementar pseudonimização para ensaios clínicos
- Deploy DLP com foco em fórmulas patenteadas

- MFA obrigatório + biometria para dados críticos
- Validar eTMF conforme requisitos EMA
- Estabelecer processo de farmacovigilância 24/7

#### 7.1.3 Fase 3: Conformidade Total (Meses 7-9)

- Completar AIPD para todos os ensaios
- Implementar SBOM para produtos com software
- Auditoria 21 CFR Part 11 + RGPD
- Certificar processos ALCOA+
- Treino de resposta a inspeções FDA/EMA

#### 7.1.4 Fase 4: Maturidade e Melhoria Contínua (Meses 10-12)

- SIEM com correlação para deteção de exfiltração
- Testes "motivated intruder" para anonimização
- Disaster recovery com RTO/RPO validados
- Revisão completa e preparação para CTR 2025

## 7.2 Considerações Finais e Alertas Críticos

- Retenção 25 Anos: Este requisito aplica-se a todos os ensaios que possam ser submetidos na UE, incluindo fora da Europa
- Pseudonimização diferente Anonimização: Dados pseudonimizados continuam sob o RGPD, não se pode assumir que códigos de paciente tornam os dados anónimos

## 8 Plano de Proteção

Este plano de proteção aborda a forma como a 4Pharma irá tratar os riscos identificados, reduzindo a sua exposição, quer seja através de estratégias de mitigação, transferência ou até aceitação, consoante a criticidade e o contexto de cada risco.

Para definir as medidas necessários, é essencial reconhecer quem são os potenciais agentes de ameaça (players), dado que é o perfil destes agentes que condiciona os vetores de ataque e a eficácia dos controlos a implementar. Entre os principais atores de ameaça à 4Pharma, destacam-se:

1. Concorrentes diretos, potenciais responsáveis por espionagem industrial visando fórmulas, informação estratégica ou processos de fabrico;
2. Hackers e grupos organizados, motivados por lucro, que procuram explorar vulnerabilidades técnicas para obter acesso indevido a dados sensíveis ou lançar ataques como ransomware;
3. Hacktivistas ou ativistas, que, em determinados contextos (contestação ao uso de animais em testes, anti vacinas...), podem visar a reputação e sistemas da empresa;
4. Colaboradores, ex-colaboradores ou parceiros com acesso privilegiado e potencial para causar danos intencionais ou acidentais;
5. Atores patrocinados por Estados, sobretudo em setores estratégicos como o desenvolvimento, onde existe interesse em inovação tecnológica e dados clínicos.

A identificação destes perfis é crucial para orientar as ações de proteção, garantindo que as medidas propostas respondem às ameaças mais prováveis e relevantes para o contexto da 4Pharma.

### 8.1 R01 – Roubo de Propriedade intelectual

#### *Ativo:*

- Fórmulas patenteadas

#### *Ameaças:*

- Acesso não autorizado por atacantes externos através de phishing ou exploração de vulnerabilidades nos sistemas de I&D.
- Fuga de informação por colaboradores internos, seja de forma intencional ou accidental.
- Roubo de dados via terceiros, como fornecedores ou parceiros com permissões inadequadas.

#### *Estratégia*

- Mitigar

#### *Medidas de Mitigação*

- Implementação obrigatória de autenticação multifator (MFA) em todos os acessos a sistemas críticos.
- Segmentação da rede para separar ambientes de I&D dos restantes sistemas.
- Formação regular a colaboradores sobre ameaças como phishing e engenharia social.
- Auditoria periódica aos logs de acesso e análise de atividades suspeitas.
- Estabelecimento de acordos de confidencialidade (NDA) e controlo de acessos para todos os parceiros e fornecedores.

#### *Responsável*

- CISO, Diretor de I&D.

## **8.2 R02 – Violação de Dados de Ensaios Clínicos**

#### *Ativo:*

- Dados de ensaios Clínicos

#### *Ameaças:*

- Acesso indevido ou divulgação de dados pessoais e clínicos por intrusão externa ou por erro interno.
- Exfiltração de dados através de endpoints não seguros ou má configuração de serviços cloud.

#### *Estratégia:*

- Mitigar

#### *Medidas de Mitigação:*

- Encriptação obrigatória de dados guardados e em trânsito (AES-256).
- Pseudonimização dos dados dos participantes em ensaios, assegurando que a chave é separada e protegida.
- Políticas de acesso baseadas em funções (RBAC) e revisão regular das permissões.
- Monitorização contínua de acessos, deteção de anomalias e resposta rápida a incidentes.
- Formação específica para equipas clínicas sobre confidencialidade e proteção de dados.

#### *Responsável:*

- DPO, Diretor Clínico, Diretor de TI.

### 8.3 R03 – Acesso não autorizado a Dados de Pacientes

#### *Ativo:*

- Dados de pacientes, pessoais e clínicos.

#### *Ameaças:*

- Tentativas de acesso não autorizado por atacantes externos, colaboradores internos ou terceiros, seja por meios técnicos (hacking, exploração de vulnerabilidades) ou engenharia social.
- Possibilidade de exposição accidental de dados sensíveis devido a má configuração de sistemas, erro humano, ou partilha inadvertida.
- Acesso indevido a dados de farmacovigilância, que podem conter informações identificáveis e confidenciais sobre reações adversas e tratamentos.

#### *Estratégia:*

- Mitigar.

#### *Medidas de Mitigação:*

- Restringir o acesso a dados de pacientes (ensaios, farmacovigilância) exclusivamente a pessoal autorizado e justificado, com base em princípios de RBAC (“need-to-know”).
- Encriptação dos dados guardados e em trânsito, independentemente do tipo de base de dados.
- Implementação de pseudonimização e anonimização sempre que possível, especialmente para dados de ensaios clínicos.
- Monitorização ativa dos acessos e geração de alertas para atividades anómalas ou não autorizadas.
- Sessões regulares de formação e sensibilização para todos os colaboradores que possam ter acesso a dados de saúde.
- Revisão periódica das permissões de acesso, e auditoria aos logs.

#### *Responsável:*

- DPO, Diretor de TI, Responsável de Farmacovigilância.

### 8.4 R04 – Divulgação de preços diferenciados

#### *Ativo:*

- Informação comercial, vantagem competitiva

#### *Ameaças:*

- Exposição não autorizada de listas de preços, seja por erro humano (envio errado de e-mail, partilha inadvertida) ou por ataque externo (acesso indevido ao ERP ou aos emails).
- Roubo ou divulgação por colaboradores ou parceiros comerciais com acesso a essa informação.

*Estratégia:*

- Mitigar.

*Medidas de Mitigação:*

- Implementação de políticas de controlo de acessos restritos a documentos e sistemas onde constam preços diferenciados.
- Utilização de encriptação em emails e ficheiros que contêm informação comercial diferenciadora.
- Sessões de sensibilização para os departamentos comercial e financeiro sobre o risco da partilha indevida.
- Registo e monitorização de acessos ao ERP e aos ficheiros onde estão armazenados os preços.
- Reforço das cláusulas de confidencialidade em contratos com parceiros que têm acesso a esta informação.

*Responsável:*

- Diretor Comercial, Diretor de TI

## 8.5 R05 – Comprometimento do Processo de Produção (PBF)

*Ativo:*

- Processos e sistemas de produção farmacêutica

*Ameaças:*

- Manipulação ou alteração não autorizada de parâmetros de produção, por erro humano ou sabotagem interna.
- Ataques externos a sistemas de produção, podendo resultar em alteração de fórmulas, desvio de produção, interrupção dos processos, ou roubo dos processos.
- Falhas técnicas que comprometam a integridade e rastreabilidade dos processos produtivos.

*Estratégia:*

- Mitigar

*Medidas de Mitigação:*

- Implementação de controlos de acesso rigorosos a sistemas de produção, com autenticação multifator para utilizadores administrativos.
- Segregação de funções e registo detalhado de todas as operações realizadas em sistemas críticos.
- Monitorização contínua dos sistemas de produção, com alertas para alterações não autorizadas.
- Revisão e teste regular dos planos de continuidade e restauro dos sistemas de produção.
- Formação periódica a operadores e técnicos sobre práticas seguras e resposta a incidentes.

*Responsável:*

- Diretor de Produção, Diretor de TI

## 8.6 R06 – Indisponibilidade do Sistema de Farmacovigilância

*Ativo:*

- Sistema e base de dados de farmacovigilância (registo de efeitos adversos, comunicações com entidades reguladoras)

*Ameaças:*

- Ataques de negação de serviço (DDoS) ou falhas técnicas que impeçam o funcionamento do sistema de farmacovigilância.
- Interrupção de serviço devido a avaria, erro de configuração, ou perda de ligação.
- Incidentes que impeçam a comunicação com autoridades como o INFARMED, EMA ou FDA.

*Estratégia:*

- Mitigar

*Medidas de Mitigação:*

- Garantir redundância e disponibilidade do sistema de farmacovigilância, com backups automáticos e replicação dos dados em servidores redundantes.
- Testes regulares de recuperação e falha do sistema, assegurando RTO/RPO conforme os requisitos regulatórios.
- Monitorização da disponibilidade dos serviços e alertas para a equipa técnica em caso de interrupção.
- Plano de resposta a incidentes, com procedimentos claros para canal para reportar interno e externo.

*Responsável:*

- Responsável de Farmacovigilância, Diretor de TI

## 8.7 R07 – Acesso indevido a fórmulas de genéricos

### *Ativo:*

- Fórmulas de medicamentos genéricos

### *Ameaças:*

- Acesso não autorizado por colaboradores sem necessidade de acesso.
- Fuga de informação devido a políticas de acesso menos restritivas do que nas fórmulas patenteadas.
- Possível partilha inadvertida durante operações de produção.

### *Estratégia:*

- Aceitar, considerando o menor valor estratégico das fórmulas de genéricos e a necessidade de rapidez na produção

### *Medidas complementares:*

- Caso sejam detetadas tentativas de acesso não autorizado repetidas ou incidentes, será revista a política de acesso e implementadas medidas adicionais de controlo.

### *Responsável:*

- Diretor de Produção, Diretor de TI

## 8.8 R08 – Perda de dados de colaboradores

### *Ativo:*

- Dados pessoais de colaboradores

### *Ameaças:*

- Eliminação accidental ou deliberada de registos de colaboradores por parte de utilizadores internos.
- Perda de dados devido a falha técnica em sistemas de gestão de recursos humanos.
- Possível exposição de dados sensíveis em caso de ataques externos ou ransomware.

### *Estratégia:*

- Transferir

### *Medidas de Mitigação:*

- Celebrar seguro de responsabilidade civil para cobertura de perdas de dados e danos associados.
- Estabelecimento de contratos com fornecedores de soluções de backup que garantam a proteção e recuperação dos dados.
- Políticas de backup frequentes, com testes de recuperação e validação de integridade dos dados.
- Formação ao pessoal dos Recursos Humanos sobre boas práticas na gestão e proteção dos dados.

*Responsável:*

- Diretor de RH, Diretor de TI

## 8.9 R09 – Falha em auditorias

*Ativo:*

- Processos, documentação e sistemas sujeitos a auditoria regulatória

*Ameaças:*

- Não conformidade com requisitos legais e normativos, devido a falhas em processos, documentação incompleta ou desatualizada.
- Incapacidade de responder a pedidos de auditoria em tempo útil por ausência de dados ou provas.
- Erro humano na preparação dos registos, ou falhas nos sistemas de armazenamento de documentação.

*Estratégia:*

- Mitigar

*Medidas de Mitigação:*

- Revisão periódica dos processos e documentação crítica, assegurando alinhamento com as exigências das entidades reguladoras (INFARMED, EMA, FDA, CNPD).
- Realização de auditorias internas de forma regular bem como planos de ação para correção de não conformidades identificadas.
- Implementação de sistemas de gestão documental com histórico de alterações e backups automáticos.
- Formação contínua das equipas sobre as exigências regulatórias aplicáveis.

*Responsável:*

Diretor de Qualidade, Data Protection Officer(DPO), Diretor de TI

## 8.10 R10 – Ataque Ransomware

### *Ativo:*

- Todos os sistemas e dados da organização (produção, dados farmacovigilância, dados ensaios, backups, fórmulas, sistemas de produção, sistemas laboratoriais)

### *Ameaças:*

- Ransomware realizado através de phishing, anexos maliciosos, exploração de vulnerabilidades ou dispositivos externos comprometidos.
- Encriptação de dados operacionais e/ou destruição de backups, resultando em indisponibilidade total ou parcial dos sistemas essenciais à continuidade da empresa.
- Exposição ou divulgação de dados confidenciais mediante chantagem financeira.

### *Estratégia:*

- Mitigar

### *Medidas de Mitigação:*

- Implementação de backups regulares, automáticos e testados, com cópias isoladas e offline dos dados críticos.
- Atualização e patching sistemático de todos os sistemas operativos e aplicações, incluindo endpoints e servidores.
- Utilização de soluções EDR(Endpoint Detection and Response)/antivírus avançado e firewall com regras de segmentação e deteção de comportamento anómalo.
- Formação periódica a todos os colaboradores sobre boas práticas de cibersegurança, com foco em identificação de phishing e social engineering.
- Plano de resposta a incidentes detalhado, incluindo comunicação imediata à equipa técnica e autoridades competentes em caso de infecção.

### *Responsável:*

- Diretor de TI, CISO, Comité de Segurança

## 9 Plano de Recuperação

### 9.1 Objetivo

Restaurar dados e serviços até aos RTO/POR definidos na matriz de continuidade (Cap. 6) e devolver a operação a um estado estável e validado, a partir do qual o Plano de Contingência (Cap. 10) pode assegurar continuidade e o Plano de Reposição (Cap. 11) realizar o “fail-back” para o modo normal. O foco é:

- reposição íntegra de backups verificados (hash/ALCOA+)
- reconstrução de infra-estrutura mínima viável
- conformidade com EMA/FDA/INFARMED e RGPD durante todo o processo

### 9.2 Âmbito

Abrange todos os ativos classificados como “Crítico” ou “Alto” no Cap. 4.3 (R01-R10) e na tabela de RTO/POR (Farmacovigilância, eTMF, Vault de Fórmulas, OT/SCADA, ERP, LIMS)

### 9.3 Estratégia Geral de Recuperação

Tier	Janela-alvo	Exemplos de sistemas	Local de recuperação	Tipo de backup
Platinum	≤ 15 min / ≤ 4h	Farmacovigilância, Cofres HSM	Multi-cloud ativo	Replicação síncrona + snapshots
Gold	≤ 30 min / ≤ 6h	eTMF, EDC ensaios	Cloud EU + Hot site	Backups incrementais imutáveis
Silver	≤ 1h / ≤ 8h	OT/SCADA, LIMS	Cluster OT redundante	Backups diferenciais + config script
Bronze	≤ 4h / ≤ 24h	ERP, RH SaaS	Cloud cold + stock HW	Backups full diários

## 9.4 Fases do Processo de Recuperação

Fase	Tempo-meta	Objetivos chave
R1 - Avaliação e Triagem	≤ 30 min	Confirmar natureza do incidente e ativar o nível de Tier adequado
R2 - Montagem de Dados	Variável (Tier)	1) Montar volumes read-only; 2) Validar checksums; 3) Verificar assinaturas de logs
R3 - Restauração de Serviços	Dentro do RTO	Recriar VMs/Containers, aplicar hardening básico, restaurar chaves KMS
R4 - Validação Funcional	+30 min	Smoke test de aplicações, validação ALCOA+ nos dados críticos
R5 - Handoff para Contingência	Imediato	Entregar sistemas recuperados ao Cap. 10; emitir sinal “Recuperação Concluída”

## 9.5 Guia de Recuperação por Recurso

Recurso / Tier	Ordem	Check (Validação R2)	Sub-Ordem	Ação de Recuperação (R3)	KPI / Evidência
Farmacovigilância	1	Réplica geográfica íntegra?	1.1	Se healthy, promover a réplica a primário; se lag > 15 min, re-seed da réplica	RPO ≤ 15 min
		API EudraVigilance	1.2	Forçar re-envio de lote pendente e esperar ACK	ACK ≤ 1 h
eTMF / EDC - Gold	2	Snapshot incremental último ≤ 30 min?	2.1	Montar volume read-only; executar “tmf-verify.ps1” (ALCOA+)	Hash chain validada
		Índices corrompidos?	2.2	Rebuild do índice, reindexar pesquisa	Pesquisa 100%
Vault de Fórmulas - Gold	3	Cofre em modo Lockdown?	3.1	Re-chavear KMS; reativar RBAC mínimo	Acesso auditável

		Logs imutáveis sem gaps?	3.2	Expor hash SHA-256 para SOC; arquivar em eQMS	Conformidade ALCOA+
OT / SCADA - Silver	4	Nó redundante “Ready”?	4.1	Boot no redundante; carregar firmware; aplicar “config-backup”	RTO ≤ 8h
		Sincronismo lot-ID com ERP?	4.2	Reprocessar filas; reconciliar contagens	Desvio = 0
ERP Prod. / Logística - Bronze	5	VM ativa?	5.1	Se down -> ligar; se frozen -> reboot; se falha -> restore último snapshot	RTO ≤ 24h
		SO sem erros?	5.2	Corrigir disk-check; aplicar snapshot limpo	Boot OK
		Serviço APP ativo?	5.3	Reiniciar ou redeploy WAR; se corrupção -> reinstalar	/health 200 OK
		BD online e íntegra?	5.4	Restaurar dump ≤ 30 min; re-índice	SHA-256 OK
LIMS (Gestão Laboratorial) - Silver	6	VM em cluster?	6.1	Migrar para nó saudável ou restore instantâneo	RTO ≤ 8h
		Conexão a instrumentos?	6.2	Reconfigurar drivers; validar aquisição teste	1 amostra OK
Infraestrutura de Virtualização	7	Nós hypervisor “healthy”?	7.1	Reiniciar nó; validar HA/fail-over	HA test pass
		VMs críticas acessíveis?	7.2	Restaurar snapshot ≤ 30 min	≥ 95% VMs OK
		Storage SA / NAS IOPS adequado?	7.3	Expandir pool; substituir discos	Latência / Lag < 5ms

Backups imutáveis / Sistema Central	8	Job mais recente OK?	8.1	Re-executar job falhado; analisar logs	100% jobs
		Hash dos ficheiros íntegro?	8.2	Eliminar cópia corrompida; restaurar anterior	0 erros hash
		Restore-teste file-level?	8.3	Restaurar ficheiro crítico para sandbox e validar	Teste mensal

## 9.6 Papéis e Responsabilidades (RACI)

Atividade	CISO	Dir. IT	DPO	Dir. Qualidade	Dir. Produção	Dir. Clínico
Declarar início da recuperação	A	R	C	C	I	I
Restauração de dados	C	A/R	C	C	C	C
Validação regulatória	C	C	A/R	A/R	I	A
Comunicação externa (EMA/FDA/CNPD)	I	C	A/R	C	I	A/R
Lições aprendidas	A	R	C	C	C	C

A = Accountable, R = Responsible, C = Consulted, I = Informed

## 9.7 KPIs de Recuperação

- % backups montados sem erro  $\geq 99\%$
- Tempo médio de montagem (MTTR-Data)  $\leq 45$  min (tiers Gold/Platinum)
- % de restauração validadas com hash OK = 100%
- Falhas de restauração crit. / ano  $\leq 1$
- Relatório a reguladores enviado  $\leq 48$  h (EMA/FDA) ou 72 h (CNPD)

## 9.8 Testes e Exercícios

Tipo	Frequência	Critério Sucesso
------	------------	------------------

Bare-metal - ERP	Semestral	Restore full VM ≤ 2 h; integridade BD OK
Disaster-recovery drill fármaco	Trimestral	Failover SaaS ≤ 15 min; zero perda de dados
Resistência a Ransomware	Anual	Restaurar 5 sistemas de backup imutáveis; 0 IOC* pós-verificação

\*IOC = Indicators of Compromise

## 9.9 Recursos e Ferramentas

- Backups: Veeam/Bacula (incremental-forever, GFS), object-storage WORM (S3), banda-offline trimestral.
- Infraestrutura: Hosts VMware vSphere + Kubernetes; storage SAN/NAS com latência < 5ms.
- Automação: SOAR para orquestração de playbooks, Pakcer/IaC para rebuild rápido.
- Stock HW: 10% peças críticas (UPS, discos, RAM) em armazém on-site

## 9.10 Integração com Contingência e Reposição

- Trigger: quando o Cap. 10 isola o incidente e solicita “Recuperação Tier X”.
- Handoff: ao concluir a Fase R4, emite-se sinal “Recuperação Concluída” -> Contingência ajusta carga; após Fase R5, Cap. 11 assume Reintegração Operacional.

# 10 Plano de Contingência

## 10.1 Objetivo

Os planos de contingência existem para garantir que as funções empresariais críticas possam continuar ou ser rapidamente restauradas quando ocorrem incidentes. Definem objetivos de recuperação claros - como o tempo de inatividade máximo tolerável e os limites de perda de dados - para que as organizações possam dar prioridade aos recursos e às ações sob pressão. Ao definir manuais passo a passo, atribuir funções responsáveis e pré-organizar alternativas (locais, sistemas, fornecedores), minimizam o caos e reduzem os tempos de resposta. Igualmente, os testes e as atualizações contínuos mantêm os planos alinhados com a evolução das tecnologias, regulamentos e cenários de ameaças. Em última análise, um planeamento de contingência eficaz salvaguarda as receitas, a reputação, a conformidade regulamentar e, acima de tudo, a confiança dos pacientes, parceiros e partes interessadas.

## 10.2 Plano de contingência da 4Pharma

### 10.2.1 R01 – Roubo de Fórmulas Patenteadas

#### *Objetivo:*

- Proteger a propriedade intelectual e impedir fuga para a concorrência.

#### *Triggers:*

- Alerta DLP de exportação anómala; deteção de uso de credenciais suspeitas em vault.

#### *Procedimentos:*

- Bloquear imediatamente a conta / token via PAM.
- Ativar “Vault Lockdown Mode” nos cofres HSM.
- Iniciar auditoria forense (SOC + Legal) em  $\leq 2$  h.
- Executar failover para hot-site criptografado; re-chavear KMS.

#### *Recursos:*

- Cofres HSM redundantes, CASB, DLP.

#### *Comunicação:*

- CISO (Presidente), Diretor de I&D, Diretor Jurídico, Diretor de TI.

### 10.2.2 R02 – Violação de Dados de Ensaios Clínicos

#### *Objetivo:*

- Salvaguardar confidencialidade e integridade dos dados e cumprir requisitos regulatórios.

#### *Triggers:*

- Alarme SIEM; perda de integridade em repositório EDC.

#### *Procedimentos:*

- Isolar subnet de pesquisa (modo read-only).
- Restaurar último snapshot coerente ( $\leq 30$  min).
- Varredura EDR pós-restauro e revisão de RBAC.

#### *Recursos:*

- Backups incrementais, snapshots imutáveis, EDR, SIEM.

*Comunicação:*

- CISO (Presidente), Diretor de I&D, Diretor Jurídico, DPO, Diretor de TI.

### 10.2.3 R03 – Acesso Indevido a Dados de Pacientes

*Objetivo:*

- Proteger dados pessoais dos pacientes e cumprir RGPD.

*Triggers:*

- Alerta de acesso anómalo; falha repetida de MFA.

*Procedimentos:*

- Encerrar sessão via IdP e reset de credenciais.
- Impor MFA global temporário; reset de tokens móveis.
- Ativar playbook RGPD: notificar CNPD em ≤ 72 h; informar pacientes em ≤ 7 dias.
- Patchear vulnerabilidade explorada.

*Recursos:*

- IdP, MFA, SIEM, patch management.

*Comunicação:*

- CISO (Presidente), DPO, Responsável de Farmacovigilância, Diretor Jurídico, Diretor de TI.

### 10.2.4 R04 – Divulgação de Preços Diferenciados

*Objetivo:*

- Evitar exposição da estratégia comercial.

*Triggers:*

- Download massivo de ficheiros de pricing; alerta DRM violation.

*Procedimentos:*

- Ativar DRM “view-only” para ficheiros de pricing.
- Rever logs do sistema de gestão para identificar leak.

- Aplicar watermarking e rastrear origem.

*Recursos:*

- DRM, SIEM, ERP logs.

*Comunicação:*

- CISO (Presidente), Diretor Financeiro, Diretor Jurídico, Diretor de TI.

### **10.2.5 R05 – Comprometimento do Processo Fabril (PBF)**

*Objetivo:*

- Garantir continuidade de produção conforme GMP.

*Triggers:*

- Falha de PLC ou alerta de anomalia OT.

*Procedimentos:*

- Failover automático para cluster OT redundante (latência < 5 s).
- Equipa OT Sec on-site em ≤ 1 h.
- Validar integridade do lote em curso.
- Se perda > 10 %, destruir lote conforme GMP.

*Recursos:*

- Cluster OT redundante, sistema HA.

*Comunicação:*

- CISO (Presidente), Diretor de Produção, Diretor de Qualidade, Diretor Jurídico, Diretor de TI.

### **10.2.6 R06 – Indisponibilidade da Plataforma de Farmacovigilância**

*Objetivo:*

- Manter relatório de eventos adversos 24/7.

*Triggers:*

- Downtime > 5 min; perda de heartbeat do serviço.

*Procedimentos:*

- Cutover para instância ativa em cloud secundária via DNS failover.
- Replicar base de dados até ponto de falha; validar consistência.
- Verificar integração com EMA EudraVigilance.

*Recursos:*

- Multi-cloud active-passive, DNS steering.

*Comunicação:*

- CISO (Presidente), Responsável de Farmacovigilância, DPO, Diretor Jurídico, Diretor de TI.

### **10.2.7 R07 – Acesso Indevido a Fórmulas Genéricas**

*Objetivo:*

- Minimizar exposição apesar do baixo impacto financeiro.

*Triggers:*

- Tentativas de scraping ou download em massa.

*Procedimentos:*

- Monitorar e bloquear IPs com frequência anómala.
- Ajustar controlos WAF e rate-limiting.

*Recursos:*

- WAF, SIEM, reputação IP.

*Comunicação:*

- CISO (Presidente), Diretor de I&D, Diretor Jurídico, Diretor de TI.

### **10.2.8 R08 – Perda de Dados de Colaboradores**

*Objetivo:*

- Proteger dados pessoais dos colaboradores.

*Triggers:*

- Falha no serviço RH SaaS; alerta de corrupção de backup.

*Procedimentos:*

- Acionar seguro de ciber-riscos; contactar provedor de RH.
- Restaurar dados de backup diário off-site.
- Oferecer proteção de identidade aos colaboradores por 12 meses.

*Recursos:*

- Backups imutáveis, seguro, provedor RH.

*Comunicação:*

- CISO (Presidente), Diretor de TI, DPO, Diretor Financeiro, Diretor Jurídico.

### **10.2.9 R09 – Falha em Auditorias**

*Objetivo:*

- Manter conformidade regulatória contínua.

*Triggers:*

- Relatório de não-conformidade.

*Procedimentos:*

- Mobilizar “Tiger Team” de QA para correções (plano  $\leq 48$  h).
- Reexecutar auditoria interna conforme GxP.
- Atualizar documentação e CAPA.

*Recursos:*

QA Tiger Team, CAPA tracking.

*Comunicação:*

- CISO (Presidente), Diretor de Qualidade, Diretor de Produção, Diretor Jurídico, Diretor de TI.

### **10.2.10 R10 – Ataque Ransomware Massivo**

*Objetivo:*

- Restaurar operações essenciais sem pagar resgate.

*Triggers:*

- EDR deteta encriptação massiva; perda de disponibilidade.

*Procedimentos:*

- **Contenção (≤ 15 min):** segmentar rede, kill switch AD, bloquear SMB.
- **Erradicação (≤ 2 h):** varrer EDR, remover payload.
- **Recuperação (≤ 2 h):** restaurar servidores críticos de backups imutáveis; monitorização 24 h.

*Recursos:*

- Backups imutáveis, EDR, playbook IR.

*Comunicação:*

- CISO (Presidente), Diretor de TI, Diretor Jurídico, DPO, Diretor Financeiro.

## 11 Plano de Reposição

### 11.1 Objetivo

O Plano de Reposição estabelece como retornar, de forma ordenada e validada, do modo de contingência para o modo operacional normal, garantindo que:

- Todos os serviços críticos são restabelecidos de acordo com RTO/RPO definidos no Capítulo 4, SubCap 4.3 (≤ 2h / ≤ 30min);
- A integridade, confidencialidade e disponibilidade dos dados é comprovada segundo ALCOA+ e 21 CFR Part 11 (FDA);
- Conformidade com INFARMED, EMA, FDA e RGPD durante todo o processo;
- Lições aprendidas sejam capturadas para melhoria contínua.

### 11.2 Âmbito

Aplica-se a todos ativos com risco ≥ que 8 na matriz do Capítulo 4 (R01-R10), incluindo:

Categoria	Sistema	RTO	RPO	Regulamentação
Propriedade Intelectual	Cofres HSM, Vault de fórmulas	4h	15min	NDA, RGPD
Dados de Ensaios Clínicos	EDC, eTMF	6h	30min	CTR 536/2014

Dados de Pacientes	BD pseudonomizadas	2h	15min	RGPD
Processo Fabril (OT)	Cluster OT, SCADA	4h	1h	GMP
Plataforma Farmacovigilância	SaaS ativo	1h	10min	GVP (EMA)

### 11.3 Princípios Orientadores

1. Validação Técnica - cada reposição deve ser precedida com verificação de integridade (hashes, logs imutáveis).
2. Validação Regulamentar - evidência documental de que os dados continuam em conformidade (ALCOA+, pseudonimização).
3. Prioridade - Prioridade por criticidade clínica; nunca reabrir um serviço que possa comprometer o fármaco, paciente ou auditoria.
4. Segurança - Controlo de acessos (MFA + PAM) reativados antes do go-live.
5. Transparência - Comunicação estruturada a stakeholders internos, reguladores e, se aplicável, aos pacientes (RGPD Artigo 34.o).

### 11.4 Fases do Processo de Reposição

Fase	Janela-Alvo	Passos-Chave
F1 - Pré-Requisito	Imediato	1 Receber sinal “Contingência Concluída” do CISO 2 Confirmar disponibilidade dos backups íntegros e ambiente de teste
F2 - Validação Técnica	≤ 30 min	<ul style="list-style-type: none"> <li>• Comparar checksums / signatures</li> <li>• Teste funcional sandbox (Smoke test)</li> <li>• Revisão de logs de contingência</li> </ul>
F3 - Validação Regulatória	≤ 1h	<ul style="list-style-type: none"> <li>• Conferir ALCOA+ nos dados críticos (e.g. TMF)</li> <li>• Garantir que pseudonimização permanece intacta</li> </ul>
F4 - Reintegração Operacional	Variável, dentro do RTO	<ul style="list-style-type: none"> <li>• Cut-over controlado para produção</li> <li>• Monitorização reforçada 24h (SIEM)</li> </ul>

F5 - Encerramento e Lições	≤ 5 dias	<ul style="list-style-type: none"> <li>Post-mortem com todas as áreas</li> <li>Atualizar playbooks de contingência e reposição</li> </ul>
----------------------------	----------	-------------------------------------------------------------------------------------------------------------------------------------------

## 11.5 Procedimentos Específicos por Risco

Risco (Cap. 11)	Trigger de Reposição	Procedimentos Chave	Evidência de Conclusão
R01 - Roubo de PI	“Vault Lockdown Mode” levantado	Re-chavear cofres KMS, restaurar controlo RBAC, reabrir acesso apenas após dupla revisão CISO + Dir. I&D	Relatório forense assinado
R02 - Violação de Dados de Ensaios	Snapshot restaurado OK	Novas verificações SHA-256, validação de integridade de protocolo de estudo, envio de nota de restauro às CROs	Conferência CRO aceita
R03 - Dados de Pacientes	Playbook RGPD finalizado	Recomposição de tokens MFA, revisão de consentimentos, relatório à CNPD	Ofício CNPD arquivado
R05 - OT / PBF	OT-cluster de volta a primário	Teste em vazio de linha; certificação QA lote em curso	Form GMP-QA-PBF-02
R10 - Ransomware	Decisão “clean-room” OK	Restaurar VMs a partir de backups imutáveis; varrimento EDR pós go-live	Log SIEM sem IOC 24h

## 11.6 Guia de Reposição

Recurso / Serviço	Ordem	Verificação / Check	Sub-Ordem	Ação de Reposição	Observações / KPIs
ERP (Produção & Logística)	1	VM ERP ativa?	1.1	Se a VM estiver down, ligar manualmente; se estiver “frozen”, forçar reboot no hypervisor.	RTO ≤ 4h

		SO inicia sem erros?	1.2	Corrigir disk-check; Aplicar snapshot limpo se falhar	Log boot validado
		Serviço da app (Tomcat / ISS) ativo?	1.3	Reiniciar serviço; se falha -> redeploy WAR ou reinstalar	Teste pedido "/health" 200 OK
		DB online e íntegra?	1.4	Restaurar último dump ( $\leq$ 30 min) + reindex	Checksum SHA-256
LIMS (Gestão Laboratorial)	2	VM LIMS em cluster?	2.1	Migrar live para nó saudável ou restore instantâneo	RTO $\leq$ 4h
		Conexão a instrumentos	2.2	Rconfigurar drivers; validaar aquisições	1 amostra teste OK
		Integração ERP?	2.3	Sincronizar filas; reconciliar lotes pendentes	Zero pendências (hanged)
Farmacovigilância (DB & Portal)	3	SGDB replica OK?	3.1	Promover réplica a primário; re-seed se lag $>$ 15 min	RPO 15 min
		Sincronismo EudraVigilance?	3.2	Forçar re-envio batch; verificar ACK	ACK $\leq$ 1h
Fórmulas Patenteadas (Vault HSM)	4	Cofre em "Lockdown"?	4.1	Re-chavear KMS; reativar RBAC mínimo	Acesso auditável
		Registros de acesso íntegros	4.2	Validar logs imutáveis; exportar hash para SOC	Conformidade ALCOA+
Infraestrutura de Virtualização	5	Nós do hypervisor no estado saudável?	5.1	Reiniciar nó com falha; validar HA / failover	HA test pass
		VMs críticas acessíveis?	5.2	Se falha, restaurar snapshot $\leq$ 30min	$\geq$ 95% VMs OK
		Storage SAN / NAS com IOPS adequado?	5.3	Expandir pool ou repor discos; otimizar tiering	Latência/Lag $<$ 5 ms

Sistema de Backups / Imutáveis	6	Job mais recente concluiu OK?	6.1	Re-executar tarefa falhada; investigar logs Veeam/Bacula	100% Jobs
		Integridade hash dos ficheiros	6.2	Eliminar cópia corrompida; restaurar anterior	0 erros hash
		Restauro de teste (file-level) funciona?	6.3	Restaurar ficheiro crítico para sandbox e validar	Teste mensal
OT / SCADA (Linha Estéril)	7	PLCs em estado RUN?	7.1	Recarregar firmware; aplicar config backup	RTO ≤ 4h
		Sincronismo com ERP (lot ID)?	7.2	Reprocessar filas; reconciliar contagens	Desvio = 0
Energia e Ambiente	8	UPS autonomia > 15 min?	8.1	Trocar baterias; recalibrar BMS	Autonomia OK
		Gerador Diesel online?	8.2	Teste de arranque; atestar combustível	Teste mensal pass

## 11.7 Papeis e Responsabilidades (RACI)

Atividade	CISO	Dir. IT	DPO	Dir. Qualidade	Dir. Produção	Dir. Clínico
Autorizar início da reposição	A	R	C	C	I	I
Validação Técnica	C	A/R	C	C	C	C
Validação Regulatória	C	C	A/R	A/R	I	A
Comunicação e Reguladores	I	C	A/R	C	I	A/R
Post-mortem e Lições	A	R	C	C	C	C

A = Accountable, R = Responsible, C = Consulted, I = Informed

## 11.8 KPIs de Reposição

Métrica	Meta	Fonte
---------	------	-------

% de sistemas repostos no RTO	$\geq 95\%$	Dashboard CEO
% de dados críticos validados sem erro	100%	Relatórios de Validação F2
Nº de não-conformidades regulatórias pós-incidente	0	Auditoria QA
Prazo de envio de relatórios a reguladores	$\leq 48\text{h EMA / FDA; } \leq 72\text{h CNPD}$	Playbooks
% de recomendações de lições aprendidas implementadas	$\geq 80\%$ em 90 dias	Steering Committee

## 11.9 Testes e Exercícios

Tipo	Frequência	Escopo	Critério de Sucesso
Simulação de reposição total (full fail-back)	Anual	Todos os sistemas nível ALTO / CRÍTICO	$\geq 90\%$ passos concluídos sem desvio
Teste de reposição OT “lote em curso”	Semestral	Linha estéril	Lote aprovado por QA
Table-top regulatório (EMA / FDA)	Semestral	Dados clínicos & TMF	0 findings CRÍTICOS
Teste de verificação de hash aleatório	Mensal	10% backups	100% match

## 11.10 Requisitos de Documentação

- “Form-REP-01” - Registo de Validação Técnica
- “Form-REP-02” - Checklist de Conformidade Regulatória
- “Form-REP-03” - Acta de Reintegração Operacional
- “REP-RR-XX” - Relatório de Revisão Pós-Incidente (root-cause + ações)

Todos os formulários devem ser arquivados no eQMS sob a categoria Business Continuity / Reposição e retidos por 10 anos (ou 25 anos para dados de ensaios).

## 11.11 Requisitos de Recursos

- Pessoal: 2 técnicos IT, 1 analista SIEM (SOC), 1 QA, 1DPO-adjunto on-call.
- Tecnologia: Ambiente de teste isolado, ferramentas de validação de integridade, SIEM integrado, PAM, licenças EDR.
- Orçamento estimado 2025: € 300k

## 12 Plano de Ação Imediata (Fire-Drill)

### 12.1 Objetivos

- Proteger pessoas, pacientes e ativos críticos.
- Conter rapidamente o incidente para limitar impacto.
- Ativar a cadeira de resposta (Cap. 9 -> 10 -> 11).
- Garantir comunicação clara a todas as partes interessadas (internas, reguladoras, clientes).

### 12.2 Âmbito

Categoria	Exemplos	Nível de Ação
Ciber	Ransomware, fuga de fórmulas, DoS a farmacovigilância	Fire-Drill
OT / Produção	Paragem de linha estéril, contaminação automáticas detectada	Fire-Drill
Dados clínicos	Violação de DB eTMF, suspeita de re-identificação	Fire-Drill
Segurança Física	Incêndio em Data-Center, falha de UPS prolongada	Fire-Drill

### 12.3 Princípios-Chave

1. Golden Hour - As decisões tomadas nos primeiros 60 min têm maior impacto TCO e na reputação.
2. Cointain -> Communicate -> Coordinate (3C)-
3. Safety First - Pessoas antes de sistemas.

4. Regulatory Clock - RGPD 72 h, EMA/FDA 24 - 48 h: o cronómetro inicia-se no detection time.
5. One Source of Truth - War Room + Teams “Fire-Drill-Live”; evitar canais paralelos.

## 12.4 Fluxo de Ação

T-0 ~ 15 min	T-15 ~ 30 min	T-30 ~ 60 min	T > 60 min
<b>DETECT &amp; ALERT</b> <ul style="list-style-type: none"> <li>• Qualquer colaborador aciona Fire-Drill via número 7777 ou botão SIEM.</li> <li>• SOC abre ticket #FD-YYYY-NN</li> </ul>	<b>ASSESS &amp; CONTAIN</b> <ul style="list-style-type: none"> <li>• Gestor de Crise (on-call) confirma severidade.</li> <li>• Aciona Playbook “Isolate” (seregar rede, bloquear conta, travar OT).</li> </ul>	<b>INITIATE PLANS</b> <ul style="list-style-type: none"> <li>• Ativa Equipa de Incidente (tab 12.5).</li> <li>• Decide se entra em Cap. 9 Recuperação.</li> <li>• Comunicação inicial: “holding statement” a Dir. Comunic.</li> </ul>	<b>ESCALATE &amp; TRANSITION</b> <ul style="list-style-type: none"> <li>• Se criticidade ≥ High, acionar Contingência (Cap. 10).</li> <li>• Se dados pessoais, DPO inicia notificação CNPD.</li> <li>• Preparar hand-off para Cap. 11 Reposição</li> </ul>

## 12.5 Estrutura da Equipa de Incidente (Incident Command)

Função	Nome (24 x 7 rota)	Responsabilidades
Incident Commander	CISO ou suplente	Tomada de decisões; autoriza comunicação externa
Gestor Técnico	Dir. IT (infra)	Coordena SOC, equipa redes/Cloud
Gestor OT	Dir. Produção	Contenção em PLC/SCADA
DPO	...	Avalia impacto RGPD; notificação CNPD
Gestor Clínico	Dir. Ensaios	Dados paciente / eTMF
Comunicação	Dir. Comunic. Corp.	Press release, canais internos
Regulatório / Farmacovigilância	QA Head	Interface EMA / FDA / INFARMED

Sec. De War-Room	PMO BCP	Regista tempos, ações, lições
------------------	---------	-------------------------------

## 12.6 Check-List “Go / No Go” para conter Sistema Afetado

Pergunta	Sim -> Fazer	Não -> Fazer
Vemos tráfego anómalo ativo?	Isolar interface, remover da VLAN	Verificar logs das últimas 24h
Há risco imediato a pacientes / produção?	Parar linha / bloquear API	Manter monitorização reforçada
Backup imutável mais recente íntegro?	Sinalizar “OK-Backup”	Acionar snapshot de emergência
Autenticação comprometida?	Reset de credenciais + MFA	Forçar rotação em 4h

(Checklist impresso nos Data-Centers e OT-rooms)

## 12.7 Comunicação - modelos rápidos

- Teams / War-Room - Canal “Fire-Drill-Live” (participação forçada a membros 12.5).
- Holding-Statement ( $\leq 1$ )

“Estamos a investigar um incidente que afeta parte dos nossos sistemas. As operações críticas permanecem seguras. Atualizaremos dentro de 60 min.”

- Status-Page Pública - rótulos “Investigating” -> “Identified” -> “Mitigating” -> “Resolved”.
- Templates Regulatórios (EMA, FDA, CNPD) pré-carregados em ServiceNow para submissão rápida.

## 12.8 Critérios de Encerramento do Fire-Drill

1. Root-Cause identificado ou workaround estabilizado;
2. Nenhum risco residual crítico (ALCOA+, GMP, RGPD) em aberto;
3. Hand-off formal a Cap.9 Recuperação ou, se já finalizado, diretamente para Contingência/Reposição;
4. Comunicado final emitido;
5. Post-mortem marcado ( $\leq 5$  dias).

## 12.9 KPIs do Fire-Drill

Métrica	Meta
Mean-Time-to-Detect (MTTD)	≤ 15 min
Mean-Time-to-Contain (MTTC)	≤ 30 min
First Public Statement	≤ 60 min
Incidentes “Critical” por ano	≤ 2
Lições implementadas em 90 d	≥ 80%

## 12.10 Integração com os restantes planos

- Fire-Drill = gatilho inicial - foca-se em detection, contenção e primeira decisão.
- Se o evento ultrapassar 60 min ou impactar RTO/POR -> Plano de Recuperação (Cap. 9).
- Se serviços precisarem de mover para infraestrutura secundária -> Contingência (Cap. 10).
- Quando ambiente estabilizar e for seguro voltar -> Reposição (Cap. 11).

## 12.11 Revisão e Treino

- Exercício completo “Fire-Drill-Day” trimestral (inclui SOC, OT, Clínico).
- Exercício “table-top” mensal (1h) focado em decisão 3C.
- Atualização anual do capítulo após auditoria externa ou sempre que ocorrer um incidente real.

## 13 Conclusão

Este plano de segurança representa um compromisso sério da 4Pharma com a proteção dos seus ativos mais valiosos, desde a propriedade intelectual que impulsiona a inovação, até aos dados pessoais que lhe são confiados tanto por pacientes quer por colaboradores.

A implementação bem-sucedida requer não apenas investimento financeiro, mas uma mudança cultural que coloca a segurança no centro das operações, com o apoio e sensibilidade da gestão, a disponibilização de recursos adequados, e principalmente o empenho dos colaboradores, a 4Pharma pode não apenas cumprir as suas obrigações regulamentares, como almejar tornar-se um exemplo de excelência em segurança no setor farmacêutico.

O percurso será deveras desafiante, mas os benefícios; proteção dos pacientes, salvaguarda da inovação, e sustentabilidade do negócio, justificam o esforço.

## 14 Anexos

### A. Arquitetura / Flow do sistema e/ou negócio (Explicação) – Imagem via Napkin (Light / Dark)



## ANEXO

### A - Mapeamento NIST 800-14

<b>Princípio NIST</b>	<b>Implementação 4Pharma</b>
1. Suporte da Missão	Segurança alinhada com objetivos farmacêuticos
2. Elemento Integral	Segurança em todas as fases do medicamento
3. Custo-Eficácia	ROI demonstrado na proteção de PI
4. Responsabilidades Explícitas RACI definido para todos os processos	
5. Accountability	Auditoria e rastreabilidade completas
6. Avaliação Periódica	Revisões trimestrais de risco
7. Sociabilidade	Integração com parceiros do setor
8. Abordagem Abrangente	Técnica + Organizacional + Física

### B - Checklist de Conformidade RGPD

- Nomeação de DPO
- Registo de atividades de tratamento
- Base legal para cada tratamento
- Procedimentos para direitos dos titulares
- Avaliações de impacto (AIPD)
- Medidas técnicas e organizacionais
- Notificação de violações (72h)
- Contratos com subcontratantes
- Transferências internacionais
- Formação e consciencialização