Associação Portuguesa de Empresas de Distribuição

# MANUAL DE BOAS PRÁTICAS DE CIBERSEGURANÇA PARA O SETOR DO RETALHO

Skill & Reach

Comissão de Digitalização e Cibersegurança

# MANUAL DE BOAS PRÁTICAS DE CIBERSEGURANÇA PARA O SETOR DO RETALHO

# FICHA TÉCNICA

**APED - Associação Portuguesa de Empresas de Distribuição**
Rua Alexandre Herculano, nº 23 - 3º
1250-008 Lisboa
+351 217 510 920
geral@aped.pt
aped.pt

**Data**
novembro de 2025

**Tiragem**
400 exemplares

**Design**
GBNT - Shaping Communication

**Documento elaborado em parceria com a Skill & Reach**

# ÍNDICE

1. **Introdução** ..... 4
2. **Ciber Riscos para a Distribuição** ..... 5
3. **Princípios Fundamentais** ..... 7
   3.1. Fase 1: Analogia do Castelo ..... 7
   3.2. Fase 2: Medidas de Cibersegurança Reforçadas ..... 10
   3.3. Fase 3: Alinhamento com Referenciais de Mercado ..... 11
4. **Gestão de Incidentes** ..... 13
   4.1. Fases da Gestão de Incidentes ..... 13
   4.2. Princípios-Chave ..... 15
5. **Enquadramento Legal** ..... 16
   5.1. Diretivas Europeias ..... 16
      5.1.1. Diretiva de Segurança de Redes e Informações (SRI/ NIS2) ..... 16
      5.1.2. Diretiva de Resiliência das Entidades Críticas (REC /CER) ..... 19
   5.2. Regulamentos Europeus ..... 20
6. **Evolução da Maturidade em Cibersegurança** ..... 21
7. **Recursos Úteis** ..... 23
   7.1. Apoio Direto ..... 23
   7.2. Recursos de Consulta ..... 24
      7.2.1. Recursos Nacionais ..... 24
      7.2.2. Recursos Internacionais ..... 24
      7.2.3. Plataformas de Formação e Sensibilização ..... 25
8. **Conclusão** ..... 26
9. **Anexo** ..... 27
   9.1. Checklist ..... 27

# 1. INTRODUÇÃO

A transformação digital trouxe novas oportunidades para o setor da distribuição, mas também uma exposição crescente a ciber riscos.

O retalho e a distribuição dependem cada vez mais de sistemas digitais para gerir cadeias de abastecimento, pagamentos, logística e relação com clientes. Esta digitalização aumenta a eficiência, mas também abre portas a ataques informáticos que podem afetar a confiança dos consumidores, interromper operações críticas e causar perdas financeiras significativas. A cibersegurança deixou de ser apenas uma responsabilidade da área de tecnologia. Hoje, é um tema transversal que envolve pessoas, processos e tecnologia.

O objetivo deste manual é apoiar as empresas associadas da APED na criação de uma cultura de boas práticas em cibersegurança, com foco na prevenção, deteção e resposta a ameaças. Pretende-se oferecer orientações práticas, alinhadas com referências nacionais e internacionais, que ajudem as organizações a proteger os seus ativos, clientes e operações.



# 2. CIBER RISCOS PARA A DISTRIBUIÇÃO

O setor da distribuição (alimentar e não alimentar, retalho e grossista) é altamente dependente de sistemas digitais para gerir operações logísticas, transações financeiras, inventário, fornecedores e interação com clientes.

Esta digitalização traz ganhos de eficiência e competitividade, mas expõe igualmente as organizações a ciber riscos significativos, que podem comprometer a continuidade do negócio e a confiança do consumidor.

Entre os principais ciber riscos para o setor destacam-se:

***Ransomware* e indisponibilidade de sistemas críticos:** Ataques que criptografam a informação em Sistemas de Informação, nomeadamente em Servidores e Estações de Trabalho, tornando inacessíveis sistemas de gestão de armazéns, logística, pontos de venda ou plataformas de *e-commerce*. A recuperação dos sistemas afetados pode levar dias a meses e poderá mesmo ser impossível a reversão.

**Ataques à cadeia de abastecimento:** Exploração de vulnerabilidades em fabricantes, fornecedores ou prestadores de serviços tecnológicos, criando um efeito em cascata que pode paralisar operações.

**Fraudes digitais e engenharia social:** Campanhas de *phishing* e *Business E-mail Compromise* (BEC) direcionadas a colaboradores, levando a acessos indevidos ou transferências financeiras fraudulentas, incluindo o pagamento de faturas falsas.

**Roubo de dados de clientes e parceiros:** Acesso privilegiado a fontes de dados com informações pessoais, financeiras e comerciais são alvos atrativos, com forte impacto legal (RGPD) e reputacional em caso de violação.

**Ataques a plataformas de pagamento e pontos de venda (POS):** *Malware* ou comprometimentos de terminais de pagamento que permitem o roubo de credenciais, cartões e dados financeiros.

**Ataques de negação de serviço (DDoS):** Sobrecarga intencional de *websites*, sistemas de *e-commerce* ou corporativos tornando-os indisponíveis em períodos de elevada procura (ex.: promoções sazonais).

**Riscos associados ao uso de IoT, OT e automação:** Dispositivos inteligentes em armazéns, sistemas de transporte, sensores e equipamentos de loja que, se mal configurados, ou com vulnerabilidades exploráveis, podem ser usados como porta de entrada para atacantes.

**Impactos reputacionais e de confiança:** Mesmo incidentes de pequena escala podem gerar perda de confiança junto de consumidores e parceiros, com impacto direto nas vendas e na competitividade.

**Usurpação de identidade:** Utilização fraudulenta da identidade digital de uma organização, colaborador ou cliente, com o objetivo de ludibriar terceiros, obter dados ou realizar operações ilegítimas. Pode assumir diferentes formas:

- ***Websites* falsos:** Criação de páginas que fazem clones de lojas online ou portais institucionais de marcas conhecidas, levando os utilizadores a introduzir dados pessoais ou financeiros que resultam em fraudes.
- **Perfis falsos em redes sociais:** Contas fraudulentas que simulam a identidade da empresa ou de colaboradores para enganar consumidores, vender produtos inexistentes ou difundir campanhas maliciosas.
- **Anúncios de emprego falsos:** Publicações fraudulentas em nome da organização, usadas para recolher dados pessoais ou credenciais de candidatos.
- ***Account Takeover* (ATO):** Comprometimento de contas legítimas (*e-mail*, plataformas de *e-commerce*, redes sociais), que permite ao atacante agir em nome da vítima e realizar fraudes de forma credível.

***Defacement*:** Alteração maliciosa da aparência de *websites* institucionais ou de *e-commerce*, afetando a imagem e a reputação da organização.

**Novos riscos relacionados com a adoção de Inteligência Artificial generativa:** Utilização de *chatbots* e outras ferramentas baseadas em IA que, se não forem devidamente configurados e monitorizados, podem expor dados, induzir clientes em erro ou ser explorados para fins maliciosos.





# 3. PRINCÍPIOS FUNDAMENTAIS

A cibersegurança não depende apenas de tecnologia. *Firewalls*, antivírus ou sistemas de monitorização são essenciais, mas insuficientes se não existirem pessoas conscientes e processos definidos.

A verdadeira resiliência resulta da combinação equilibrada de tecnologia, organização e comportamento humano.

Existem referenciais internacionais e nacionais reconhecidos, como o NIST *Cybersecurity Framework*, a ISO/IEC 27001 e o Quadro Nacional de Referência para a Cibersegurança (QNRCS) do CNCS. Estes modelos fornecem bases sólidas para programas estruturados de longo prazo, mas a sua implementação exige tempo, investimento e maturidade organizacional.

Antes de chegar a essa etapa, todas as organizações devem começar por princípios básicos de ciber-higiene, medidas acessíveis e de aplicação imediata, que reduzem significativamente o risco de incidentes.

## 3.1. FASE 1: ANALOGIA DO CASTELO

Uma organização pode ser comparada a um castelo medieval. Para resistir a ataques, o castelo não dependia apenas de muralhas, mas de várias camadas de defesa que funcionam em conjunto.

As três primeiras camadas da analogia, muralhas, portões com guardas e vigilantes, correspondem, de forma simplificada, ao modelo AAA: Autenticação, Autorização e Auditoria.

Este modelo é usado para garantir que apenas pessoas autorizadas acedem aos sistemas e que todas as ações ficam registadas e podem ser analisadas.

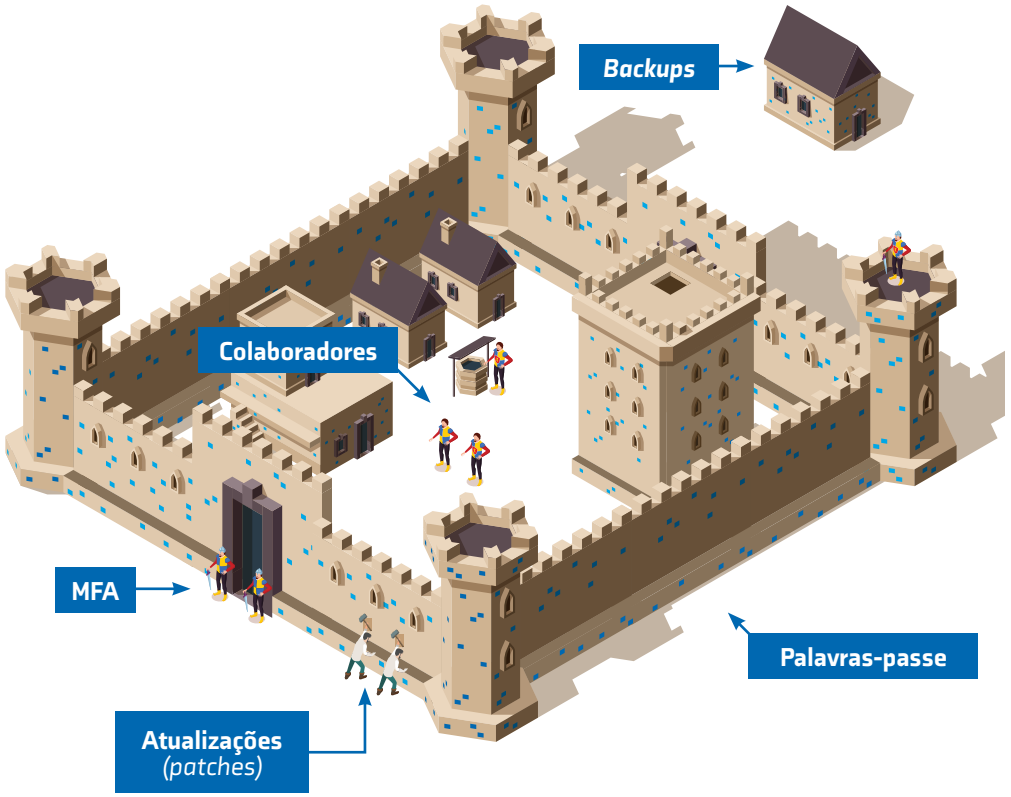


**Figura 1:** Analogia do castelo aplicada à cibersegurança

**Muralhas exteriores:** As muralhas representam a defesa perimétrica da organização, a primeira linha de proteção contra ataques vindos do exterior. Tal como as muralhas de um castelo impedem a entrada de invasores, esta camada de segurança é composta por *Firewalls* de Nova Geração, que controlam o que entra e sai da rede, e por autenticação multifator (MFA), que, para além da palavra-passe, é necessário um método adicional de autenticação. Estas medidas criam uma barreira sólida entre o ambiente interno da empresa e o mundo exterior, reduzindo o risco de intrusões.

**Portões com guardas:** Os portões simbolizam a autorização, isto é, o controlo que decide quem pode passar e até onde pode ir dentro da organização. Mesmo que alguém tenha credenciais válidas, como um colaborador com palavra-passe e autenticação multifator, pode não estar autorizado a aceder a determinadas áreas ou sistemas. Tal como num castelo, possuir a chave não basta: é preciso ter permissão para atravessar o portão. Este processo garante que cada utilizador apenas entra onde realmente deve, reforçando a segurança e o princípio do "acesso mínimo necessário".

**Vigilantes:** Os vigilantes representam os habitantes do castelo, ou seja, os colaboradores da organização. Num castelo, a segurança dependia da atenção de quem lá vivia: se os habitantes não estivessem atentos a movimentos estranhos, o inimigo poderia infiltrar-se sem ser notado. Nas empresas, acontece o mesmo, a atenção e o sentido crítico dos colaboradores são essenciais para reconhecer e reportar comportamentos suspeitos, como e-mails de origem duvidosa ou pedidos de informação fora do normal. A esta vigilância humana juntam-se os mecanismos de auditoria e monitorização, que registam e analisam automaticamente atividades anómalas. Em conjunto, esta auditoria contínua permite identificar rapidamente incidentes e reforçar a segurança de toda a organização.

**Reparação das muralhas:** Corresponde às atualizações regulares de sistemas e aplicações. Cada fissura na muralha é uma vulnerabilidade que tem de ser corrigida. A aplicação das atualizações (*patches*) de segurança, fornecidas pelos fabricantes, em computadores, servidores e restantes sistemas de rede, OT e IoT é fundamental para a ciber higiene, ao reduzir a superfície de ataque interna e externa.

**Armazéns de mantimentos:** Equivalem aos *backups* de dados. Tal como um castelo não guardava todas as reservas no mesmo local, também uma empresa não deve guardar todas as cópias de segurança dentro da própria rede. É fundamental ter backups regulares e testados, incluindo cópias externas (em *cloud* segura ou *datacenter* fora da organização), para garantir a recuperação de informação mesmo após um ataque como de *ransomware*.

**Divisão interna das áreas do castelo:** Representa a segmentação da rede informática. No castelo, áreas mais críticas eram isoladas das restantes. Do mesmo modo, os sistemas mais sensíveis, como os Pontos de Venda (POS), que incluem terminais de pagamento e *software* de faturação, os servidores de gestão (ERP) e os sistemas de armazém, devem estar separados da rede de uso geral. Isto impede que um ataque localizado se espalhe facilmente por toda a organização. A segregação de redes não implica, normalmente, custos acrescidos, pois reflete-se em arquitetura e configuração.

**Plano de defesa:** Garante que todos sabem como reagir em caso de ataque. Num castelo, uma estratégia coordenada era essencial para resistir; numa organização, o equivalente é ter um plano de resposta a incidentes, com responsabilidades definidas, pontos de contacto internos e externos, e procedimentos claros para isolar o problema e restaurar rapidamente a operação. A organização deve apostar numa estratégia de prevenção por omissão, pois o custo de um incidente é normalmente de magnitude largamente superior ao custo de uma medida preventiva.


3. PRINCÍPIOS FUNDAMENTAIS

**Comandante da defesa:** Assim como todo o castelo precisava de um responsável pela defesa, também a organização deve nomear um colaborador com a função de responsável de cibersegurança ou segurança da informação. Mesmo que seja a tempo parcial, esta figura assegura que há sempre alguém a coordenar a proteção, a supervisionar os alertas e a garantir que a cultura de ciber-higiene é eficaz.

## 3.2. FASE 2: MEDIDAS DE CIBERSEGURANÇA REFORÇADAS

Quando os fundamentos de ciber-higiene estão assegurados, a organização deve avançar para um nível superior de proteção. Nesta etapa, é essencial adotar práticas de segurança mais consistentes e sistemáticas, apoiadas em planeamento estruturado e processos internos bem definidos. Estas medidas não representam apenas um reforço, mas sim a consolidação das defesas, reduzindo riscos operacionais que podem afetar a continuidade e a resiliência do negócio.

**Política de Segurança da Informação:** Definir e formalizar um documento aprovado pela gestão que estabeleça princípios e responsabilidades em matéria de cibersegurança. Esta política deve ser comunicada a todos os colaboradores e servir de base para os processos internos e medidas técnicas de proteção.

**Inventário de ativos:** Manter uma lista atualizada de todos os equipamentos (computadores, servidores, terminais de pagamento, dispositivos móveis, equipamentos de rede, entre outros) e das aplicações utilizadas. Só é possível proteger o que está devidamente identificado. Recomenda-se que se identifiquem paralelamente os sistemas e aplicações críticos pois esses são as joias da coroa e devem ser aqueles cujo investimento em proteção deve ser maioritariamente aplicado, bem como os primeiros a serem recuperados em caso de desastre.

**Gestão de contas e acessos:** Definir e documentar processos de atribuição, revisão e remoção de acessos. Aplicar o princípio do menor privilégio e garantir registos de auditoria sobre quem acede a quê. Alinhar os processos de IT com os de RH para entrada, saída e mudança de funções de colaboradores, pois é frequente que sejam esquecidos acessos que colaboradores tinham na função antiga ou ex-colaboradores que passados meses, senão anos, ainda se mantêm ativos na organização, configurando um risco de desastre eminente.

**Segurança de *e-mail* e navegação:** Implementar filtros *anti-phishing* e *anti-spam*, bloquear anexos perigosos e reforçar a atenção para links suspeitos. O e-mail continua a ser o principal vetor de ataque nas organizações.

**Segurança física e de dispositivos:** Formalizar e aplicar regras de bloqueio de equipamentos quando não estão em uso, e políticas claras para a utilização (ou restrição) de dispositivos externos, como armazenamento USB.

**Proteção contra *malware*:** Utilizar soluções de antivírus e EDR (*Endpoint Detection & Response*) em todos os dispositivos, garantindo a sua atualização e monitorização contínua.

**Campanhas de sensibilização contínuas:** Complementar a formação com ações regulares de consciencialização (ex.: simulações de *phishing*, alertas internos, *newsletters*).

## 3.3. FASE 3: ALINHAMENTO COM REFERENCIAIS DE MERCADO

Nesta fase, a maturidade em cibersegurança passa a assentar no alinhamento com referenciais nacionais e internacionais amplamente reconhecidos. O objetivo é deixar de atuar apenas com medidas isoladas e evoluir para uma abordagem estruturada, comparável e auditável, que integre a segurança na governação da organização. Estes referenciais funcionam como guias para estabelecer políticas, processos e métricas, permitindo às organizações avaliar o seu nível de maturidade, identificar lacunas e demonstrar diligência perante clientes, parceiros e reguladores.

### Principais referenciais:

**Quadro Nacional de Referência para a Cibersegurança (QNRCS):**
Guia publicado pelo CNCS que adapta boas práticas internacionais ao contexto português. Está em processo de atualização para acompanhar a transposição nacional da Diretiva NIS2 e continuará a ser uma referência prática para apoiar as organizações na avaliação e evolução da sua maturidade em cibersegurança.

**NIST *Cybersecurity Framework* 2.0:**

Estrutura internacional que organiza a cibersegurança em cinco funções fundamentais: Identificar, Proteger, Detetar, Responder e Recuperar. Fornece orientações práticas, promove a integração da segurança na governação das organizações e sublinha a importância de medir resultados e evolução.

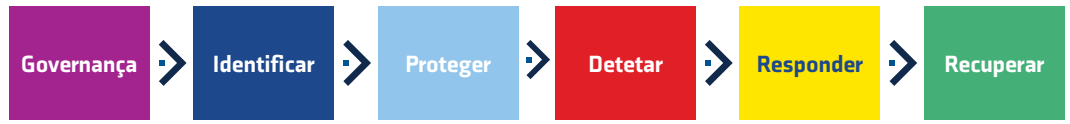


**Figura 2:** Funções NIST CSF 2.0


3. PRINCÍPIOS FUNDAMENTAIS

**ISO/IEC 27001:**
Norma internacional certificável para sistemas de gestão da segurança da informação. Define políticas e controlos estruturados e é especialmente útil para organizações que necessitam demonstrar conformidade perante clientes, parceiros ou reguladores.

**CIS *Controls* v8.1:**
Conjunto de 18 controlos de aplicação prática e imediata, organizados em três grupos de implementação (IG1, IG2 e IG3). Estes controlos permitem às organizações reforçar a sua proteção de forma gradual e proporcional aos recursos disponíveis.

Dentro dos quais destacamos as seguintes medidas:

**Monitorização contínua de segurança (SOC/SIEM):** Criar ou subcontratar serviços para Centro de Operações de Segurança (SOC) ou utilizar uma plataforna *Security Information and Event Management* (SIEM) para recolha, correlação e análise de eventos de segurança em sistemas e redes. Estas plataformas permitem identificar anomalias e gerar alertas em tempo real.

**Gestão de acessos privilegiados (PAM - *Privileged Access Management*):** Controlar contas com permissões elevadas, aplicar o princípio do menor privilégio e retirar direitos administrativos desnecessários. Isto reduz o impacto de credenciais comprometidas.

**Segmentação avançada de redes:** Além da separação básica, criar diferentes zonas de confiança (ex.: rede administrativa, rede de clientes, rede operacional/logística), limitando a propagação de ataques.

**Criptografar dados sensíveis:** Proteger informação crítica, tanto em trânsito (envio de dados entre sistemas) como em repouso (armazenamento em bases de dados ou sistemas de ficheiros em servidores), reduzindo o impacto de acessos não autorizados.

**Testes de segurança regulares:** Realizar auditorias técnicas, testes de penetração para avaliar a resiliência da organização:

- **Testes de penetração (*pentests*):** Execução de ataques controlados sobre sistemas e aplicações, por profissionais certificados, com o objetivo de identificar vulnerabilidades técnicas antes que sejam exploradas por atacantes.





# 4. GESTÃO DE INCIDENTES

Mesmo com boas práticas de prevenção, nenhum sistema é totalmente imune a ciberataques. Um incidente de cibersegurança com impacto pode comprometer operações críticas, como pontos de venda, sistemas de armazém ou plataformas de *e-commerce*, afetando diretamente a continuidade do negócio e a confiança dos consumidores.

Por isso, todas as organizações devem dispor de um plano de resposta a incidentes, que assegure uma reação rápida, coordenada e eficaz.

## 4.1. FASES DA GESTÃO DE INCIDENTES

A gestão de incidentes deve seguir cinco fases fundamentais:

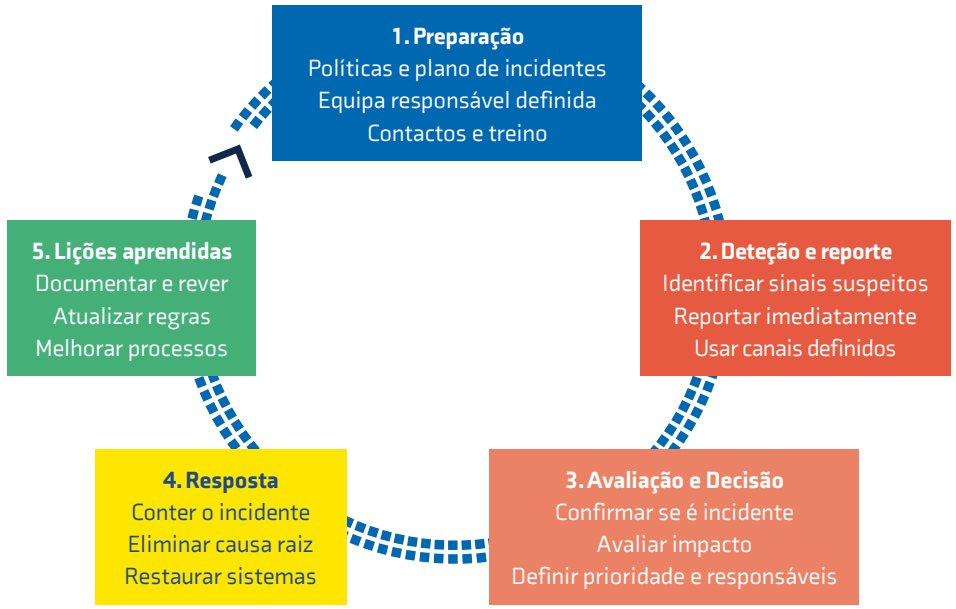


**Figura 3:** Fases da gestão de Incidentes ISO/IEC 27035

### 1. Preparação

- Ter regras e planos documentados para lidar com incidentes.
- Criar uma equipa de gestão de incidentes (com funções e contactos definidos).
- Garantir que existem ferramentas e processos de suporte.
- Realizar ações de sensibilização e treino para todos os colaboradores.
- Testar regularmente o plano de incidentes para confirmar que funciona.

### 2. Detetar e Reportar

- Monitorizar sistemas e redes para identificar sinais suspeitos.
- Permitir que qualquer colaborador reporte algo estranho de forma simples e rápida.
- Recolher informação básica sobre o que foi observado (quando, onde, como).
- Garantir que todos sabem para onde devem enviar o alerta.

### 3. Avaliar e Decidir

- A equipa analisa os eventos reportados e decide se são incidentes.
- Avalia a gravidade e o impacto (pequeno, médio ou grande).
- Define prioridades de resposta e aciona os recursos necessários.
- Documenta as decisões tomadas e quem ficou responsável por agir.

### 4. Responder

- Controlar o incidente (isolar sistemas afetados, bloquear acessos).
- Eliminar a causa do problema (remover *malware*, aplicar correções, fechar vulnerabilidades).
- Restaurar sistemas e serviços de forma controlada.
- Manter registos de tudo o que foi feito.

### 5. Lições Aprendidas

- Rever o incidente: o que funcionou bem, o que falhou.
- Atualizar planos, regras e contactos de resposta a incidentes.
- Incorporar as melhorias no processo de gestão de riscos.
- Partilhar aprendizagens com a equipa para aumentar a preparação futura.



## 4.2. PRINCÍPIOS-CHAVE

- **Rapidez na deteção e reporte:** Quanto mais cedo um incidente é identificado e comunicado, menor será o impacto nas operações e nos clientes.
- **Coordenação entre equipas:** Todas as áreas da organização, bem como fornecedores e parceiros críticos, devem conhecer o seu papel e colaborar de forma integrada.
- **Clareza nos procedimentos e na comunicação:** As instruções devem estar documentadas, ser de fácil compreensão e incluir tanto a comunicação interna como externa.
- **Melhoria contínua:** Exercícios regulares e análises pós-incidente são cruciais para reforçar a capacidade de resposta e evitar que os mesmos erros se repitam.

# 5. ENQUADRAMENTO LEGAL

A cibersegurança no setor da distribuição está enquadrada por um conjunto de instrumentos legais que estabelecem requisitos obrigatórios, tanto a nível europeu como nacional. Para as empresas associadas da APED, conhecer este enquadramento é essencial para assegurar conformidade e evitar sanções.

## 5.1. DIRETIVAS EUROPEIAS

As diretivas definem objetivos obrigatórios para os Estados-Membros, mas a sua aplicação depende da transposição para a legislação nacional.

### 5.1.1. Diretiva de Segurança de Redes e Informações (SRI/ NIS2)

A Diretiva NIS2 (UE 2022/2555) é uma diretiva que estabelece as regras europeias para reforçar a cibersegurança em setores essenciais e importantes. O seu objetivo é alcançar um nível elevado e comum de segurança de redes e sistemas de informação em toda a União Europeia, reforçando a resiliência de setores considerados essenciais e importantes para o funcionamento da sociedade e da economia. Em Portugal, a proposta de lei foi aprovada em Conselho de Ministros a 6 de fevereiro de 2025 e a todo o momento será transposta para lei nacional, que substituirá o Decreto-Lei n.º 65/2021 (transposição da primeira NIS).

A NIS2 alarga o âmbito da NIS original, passando a abranger setores como o retalho, a distribuição e a logística. Reforça a responsabilidade da gestão de topo, que passa a ter deveres formais de supervisão. Introduz a obrigação de avaliar riscos na cadeia de fornecimento e impõe regras mais rigorosas de reporte de incidentes. Por fim, estabelece um regime sancionatório mais severo, com coimas significativamente mais elevadas.

#### 5.1. 1. 1. Entidades Abrangidas no Setor da Distribuição

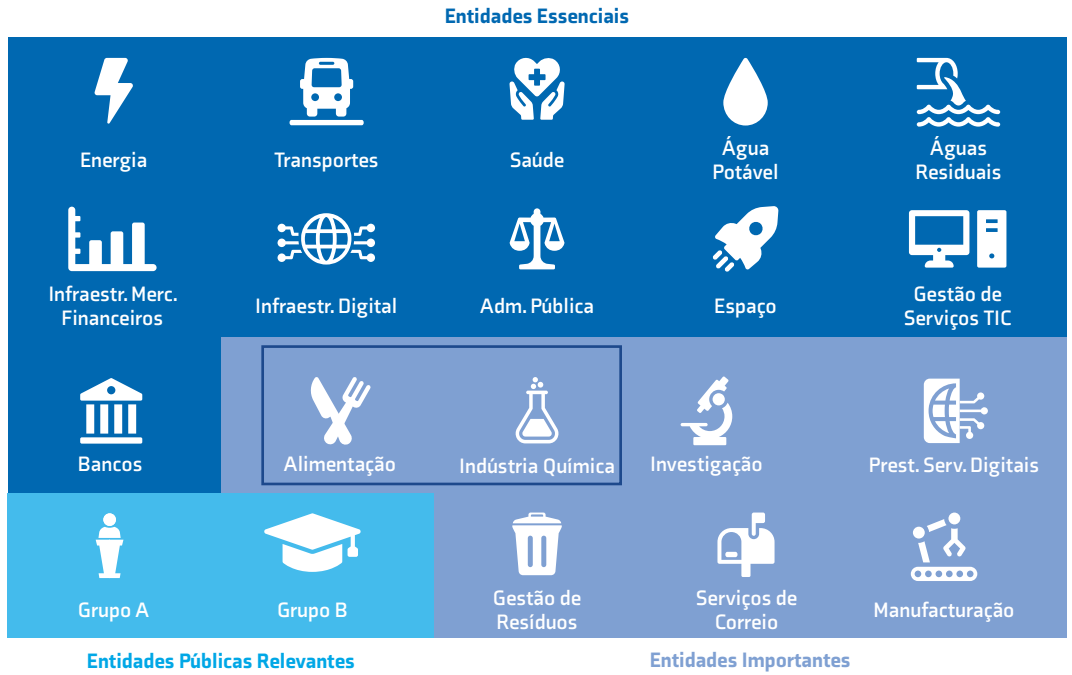


**Figura 4:** Entidades abrangidas NIS2

De acordo com a proposta de lei portuguesa, a distribuição é considerada em dois subsetores principais:

- **Alimentar:** Abrangendo empresas de distribuição grossista e de produção e transformação industriais.
- **Químico:** Abrangendo empresas de distribuição de substâncias e misturas, referidas no artigo 3.º, pontos 9 e 14, do Regulamento (CE) n.º 1907/2006 do Parlamento Europeu.

Para estes setores, a aplicação da NIS2 incide sobre empresas de média e grande dimensão, tal como definidas pela Recomendação 2003/361/CE da Comissão Europeia.

Embora a proposta de lei identifique de quais as entidades diretamente abrangidas no setor da distribuição, é importante sublinhar que também impõe a avaliação de riscos na cadeia de fornecimento.

Isto significa que empresas que não se enquadram no âmbito definido (por exemplo, pequenas empresas ou entidades que não operam diretamente na distribuição grossista) podem, ainda assim, ser afetadas se forem terceiros ou prestadores de serviços para organizações abrangidas.

Assim, mesmo empresas não abrangidas diretamente podem ser chamadas a demonstrar práticas de cibersegurança adequadas, como condição contratual imposta pelas entidades abrangidas, por serem parte integrante da cadeia de fornecimento.

#### 5.1. 1. 2. Principais requisitos

As empresas da distribuição que estão abrangidas passam a ter de cumprir um conjunto de obrigações legais em cibersegurança. Estas responsabilidades agrupam-se em cinco áreas centrais, que representam o que cada organização tem de assegurar no dia a dia:

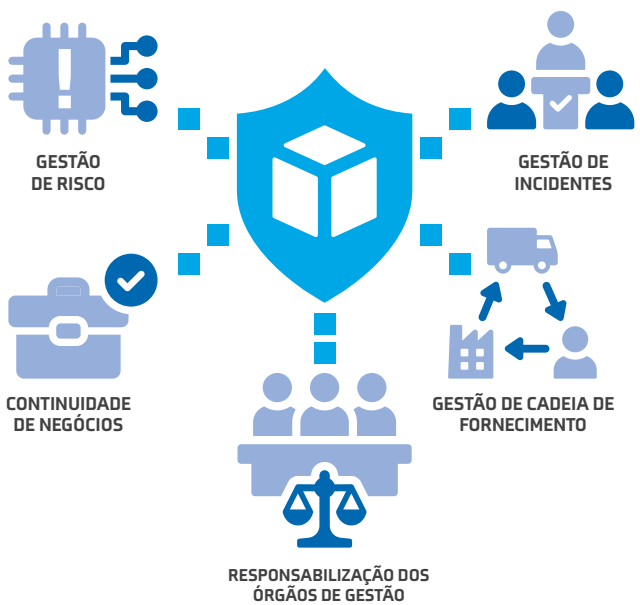


**Figura 5:** Obrigações legais das Empresas abrangidas

**Responsabilização dos Órgãos de Gestão:** A administração deve aprovar políticas, supervisionar a sua aplicação e garantir recursos adequados. A proposta de lei prevê responsabilidade direta por falhas graves, reforçando o papel ativo da gestão.

**Gestão da Cadeia de Fornecimento:** As empresas têm de avaliar e monitorizar os fornecedores, garantindo que cumprem padrões de segurança. Cabe-lhes mitigar riscos que possam comprometer a cadeia de abastecimento.

**Gestão de Incidentes:** É obrigatório ter processos claros para deteção, resposta e notificação de incidentes. Inclui reporte ao CNCS nos prazos definidos, bem como treino das equipas para reagir com rapidez.

**Gestão de Risco:** As organizações devem implementar sistemas formais para identificar, avaliar e mitigar riscos de cibersegurança, incluindo análises periódicas e relatórios.

**Continuidade de Negócio:** As entidades devem assegurar que, mesmo em caso de incidente grave, conseguem manter funções críticas e recuperar rapidamente operações essenciais, recorrendo a planos testados de continuidade e recuperação.

#### 5.1. 1. 3. Autoridade Nacional

O Centro Nacional de Cibersegurança (CNCS) é a autoridade nacional competente, responsável por coordenar a implementação da lei, apoiar as entidades abrangidas e operar o CERT.PT, que recebe notificações de incidentes e fornece assistência técnica.

### 5.1.2. Diretiva de Resiliência das Entidades Críticas (REC /CER)

A Diretiva CER (UE 2022/2557) visa reforçar a capacidade dos Estados-Membros de proteger infraestruturas essenciais de ameaças. Esta diretiva foi transposta em Portugal resultando no Decreto-Lei n.º 22/2025. Entre os setores abrangidos está a produção. tranformação e distribuição de produtos alimentares, o que significa que operadores logísticos e distribuidores alimentares de grande escala ligados ao abastecimento nacional podem vir a ser incluídos na lista nacional de entidades críticas, que será concluída até julho de 2026. Para a maioria das empresas associadas, o impacto será indireto, mas acompanhar este processo é fundamental para garantir alinhamento com futuras obrigações.


5. ENQUADRAMENTO LEGAL

## 5.2. REGULAMENTOS EUROPEUS

Os regulamentos são de aplicação direta e uniforme em todos os Estados-Membros, sem necessidade de transposição para a lei nacional.

**Regulamento DORA (UE 2022/2554):** Aplica-se a instituições financeiras e a prestadores de TIC críticos para esse setor. No contexto da APED, o impacto é apenas indireto: algumas empresas podem ser abrangidas se oferecerem serviços financeiros associados, como cartões de crédito de fidelização, crédito ao consumo ou integrações com *fintechs*. Para a maioria dos associados, o DORA não é aplicável de forma direta, mas pode gerar obrigações através de parcerias financeiras ou tecnológicas.

**Regulamento Geral de Proteção de Dados (RGPD, UE 2016/679):** É aplicável a todas as organizações que tratem dados pessoais. Para a distribuição, abrange dados de clientes, colaboradores e fornecedores. Impõe obrigações de proteção, direitos dos titulares e reporte de violações à CNPD.





# 6. EVOLUÇÃO DA MATURIDADE EM CIBERSEGURANÇA

A evolução da maturidade em cibersegurança deve ser entendida como um percurso progressivo.Cada fase acrescenta novas camadas de proteção, governação e resiliência, permitindo que as organizações passem do essencial para práticas avançadas e certificáveis.

### Fases de Evolução

**Figura 6:** Fases de Evolução da Maturidade em Cibersegurança

### Fase 1: Fundamentos

Implementação das medidas básicas de ciber-higiene, como fator múltiplo de autenticação (MFA), *backups* regulares, aplicação de atualizações (*patches*) e sensibilização dos colaboradores. O objetivo é criar a primeira barreira de defesa contra ameaças comuns.

### Fase 2 - Estruturação

A segurança começa a ser formalizada em políticas e processos, com inventário atualizado de ativos, gestão de acessos, *hardening* de sistemas e fluxos de reporte. A cibersegurança passa a estar integrada no funcionamento da organização.

### Fase 3 - Integração

A maturidade nesta fase traduz-se na adoção de uma abordagem estruturada e comparável, em que a cibersegurança passa a estar guiada por referenciais nacionais e internacionais. Este alinhamento permite integrar a segurança na governação, medir evolução de forma objetiva e demonstrar conformidade perante clientes, parceiros e reguladores.

**Fase 4 - Consolidação**

O nível mais elevado de maturidade, em que a organização valida e demonstra a sua resiliência. Inclui certificação em normas reconhecidas (ISO/IEC 27001), plano de resposta a incidentes formalizado e testado, participação em exercícios internacionais (ex.: *Cyber Europe*, promovido pela ENISA) e integração em comunidades de partilha de informação (ex.: ISAC Retalho e Distribuição). Esta etapa reforça a credibilidade externa da organização e traduz-se numa vantagem competitiva no mercado.





# 7. RECURSOS ÚTEIS

Para além deste manual, existem diversos recursos nacionais e internacionais de acesso gratuito que podem apoiar as organizações na implementação e melhoria contínua das suas práticas de cibersegurança.

## 7.1. APOIO DIRETO

Quando uma organização enfrenta um incidente de cibersegurança, é essencial saber **a quem recorrer de imediato** para obter apoio especializado. Em Portugal, existem entidades oficiais com linhas de contacto dedicadas, capazes de prestar assistência técnica, receber queixas-crime ou acompanhar situações de violação de dados pessoais.

**Centro Nacional de Cibersegurança (CNCS / CERT.PT)**
Autoridade nacional responsável pela coordenação da cibersegurança. O seu centro de resposta a incidentes (CERT.PT) apoia organizações e administrações públicas na gestão de incidentes.
cert@cert.pt
210 497 399
CNCS - Notificação de Incidentes
CNCS - Centro Nacional de Cibersegurança

**Polícia Judiciária – Unidade Nacional de Combate ao Cibercrime (UNC3T)**
Unidade especializada na investigação de cibercrime. É o ponto de contacto para crimes digitais como fraude online, *ransomware* ou roubo de dados.
211 967 000
Polícia Judiciária

**Comissão Nacional de Proteção de Dados (CNPD)**
Autoridade independente que supervisiona a aplicação do RGPD. Deve ser notificada em caso de violação de dados pessoais.
geral@cnpd.pt
213 928 400
https://www.cnpd.pt

## 7.2. RECURSOS DE CONSULTA

Para além das linhas de apoio direto, existem também guias, plataformas e iniciativas de sensibilização que ajudam as organizações a reforçar práticas de cibersegurança, aumentar a maturidade e formar os seus colaboradores. Estes recursos são gratuitos e amplamente reconhecidos a nível nacional e internacional.

### 7.2.1. Recursos Nacionais

**CNCS – Centro Nacional de Cibersegurança**

Guias, recomendações e alertas de cibersegurança adaptados ao contexto português.
https://www.cncs.gov.pt

**Polícia Judiciária – Unidade Nacional de Combate ao Cibercrime**

Orientações para reporte de incidentes de cibercrime.
https://www.policiajudiciaria.pt

**ISAC Retalho e Distribuição**

Estrutura nacional dinamizada pelo CNCS, que reúne grandes empresas do setor (como Auchan, Jerónimo Martins, LIDL, Leroy Merlin, Sonae MC), e promove a partilha de ameaças, vulnerabilidades e boas práticas.
https://www.cncs.gov.pt/pt/comunidades-cibersegurança/isacs/retalho/

### 7.2.2. Recursos Internacionais

**ENISA: Agência Europeia para a Cibersegurança**

Guias e relatórios sobre cibersegurança na União Europeia.
https://www.enisa.europa.eu

**Retail & Hospitality ISAC**

Rede internacional de partilha de informação sobre ameaças e riscos no setor do retalho.
https://rhisac.org

### 7.2.3. Plataformas de Formação e Sensibilização

**STOP. THINK. CONNECT.**

Campanha internacional de sensibilização para cibersegurança.
https://www.stopthinkconnect.org

**Coursera / edX / FutureLearn:**

Cursos gratuitos de cibersegurança de universidades internacionais.

**TryHackMe / Cyber Security Challenge PT:**

Plataformas práticas de treino em segurança digital.

**ENISA - Raising Awareness e AR-in-a-Box:**

Campanhas e *toolkit* para criação de programas internos de sensibilização.
https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns
https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box


7. RECURSOS ÚTEIS

# 8. CONCLUSÃO

A transformação digital trouxe enormes oportunidades de crescimento e eficiência para o setor da distribuição, mas também elevou o nível de exposição a ciber riscos que não podem ser ignorados. Este manual pretende demonstrar que a cibersegurança não depende apenas de tecnologia: exige igualmente processos bem definidos, colaboradores conscientes e uma cultura organizacional orientada para a resiliência.

As empresas associadas da APED devem encarar a cibersegurança como um percurso de evolução contínua. O primeiro passo dá-se pela adoção de práticas básicas de ciber-higiene, acessíveis e de impacto imediato. A partir daí, a maturidade deve crescer através da formalização de políticas e processos, até chegar ao alinhamento com referenciais de mercado.

O enquadramento legal europeu e nacional, em particular a transposição da Diretiva NIS2, estabelece novas responsabilidades para o setor da distribuição. Este contexto reforça a necessidade de uma abordagem estruturada, capaz de demonstrar conformidade, assegurar continuidade de negócio e proteger a cadeia de abastecimento.

Para as organizações associadas da APED, este caminho representa benefícios tangíveis: redução de incidentes, maior continuidade das operações, confiança reforçada de clientes e parceiros e, sobretudo, vantagem competitiva num setor altamente exigente.

**A cibersegurança deve ser encarada como um investimento estratégico e contínuo, capaz de proteger não apenas dados e sistemas, mas também a reputação e o futuro sustentável das organizações.**



# 9. ANEXO

## 9.1. CHECKLIST

### Medidas Básicas de Ciber-Higiene – Fase 1

| | |
|---|---|
| **Palavras-passe fortes e únicas** (*preferência: gestor de senhas*) | |
| **MFA ativada em contas críticas** | |
| **Backups regulares e testados, incluindo cópias fora da organização** | |
| **Atualizações de software e patches aplicados** | |
| **Segmentação da rede** *(ex.: POS separado da rede geral)* | |
| **Sensibilização dos colaboradores** *(phishing, uso de dispositivos)* | |
| **Definição de um Responsável de Cibersegurança / Segurança da Informação** | |
| **Canal interno definido para reporte de incidentes** *(telefone, e-mail, helpdesk)* | |

### Medidas Reforçadas – Fase 2

| | |
|---|---|
| **Existência de uma política de segurança de informação** | |
| **Inventário atualizado de ativos** *(hardware, software, contas, sistemas críticos)* | |
| **Gestão de acessos pelo princípio do menor privilégio** | |
| **Remoção de contas inativas e revisão regular de permissões** | |
| **Hardening de sistemas** *(configurações seguras, serviços desnecessários desativados)* | |
| **Antivírus/EDR instalado e atualizado** | |
| **Bloqueio de dispositivos externos não autorizados** | |
| **Campanhas regulares de sensibilização** *(simulações de phishing, newsletters)* | |
| **Fluxos formais de reporte interno e externo** *(CNCS, PJ, CNPD)* | |

### Medidas Avançadas – Fase 3

| | |
|---|---|
| Monitorização contínua de eventos e alertas de segurança *(SIEM/SOC)* | |
| Gestão de acessos privilegiados *(PAM)* | |
| Segmentação avançada de redes *(zonas de confiança distintas)* | |
| Criptografia de dados sensíveis em trânsito e repouso | |
| Testes regulares de segurança *(pentests)* | |
| Plano de resposta a incidentes formalizado e testado | |

Associação Portuguesa de Empresas de Distribuição

www.aped.pt
Rua Alexandre Herculano 23, 3º
1250-008 Lisboa • Portugal