Guia de Referência Cruzada de Conformidade NIS2 da Sepio

Resumo Executivo

A NIS2 exige que as entidades abrangidas demonstrem uma governação eficaz da cibersegurança, uma gestão de risco adequada, capacidades de reporte de incidentes e preparação para auditorias. Na prática, muitos programas falham logo no primeiro passo: manter um inventário fiável do que está efetivamente ligado ao ambiente.

A Sepio colmata essa lacuna com a validação da identidade dos dispositivos através do AssetDNA, visibilidade completa sobre ativos geridos e não geridos, controlo de acesso ao hardware baseado em políticas e fluxos de mitigação automatizados. Isto torna a Sepio especialmente relevante para os requisitos da NIS2 em matéria de gestão de ativos físicos, segurança da cadeia de abastecimento, tratamento de incidentes e eficácia dos controlos baseada em evidência.

Melhor enquadramento: para organizações que precisam de visibilidade e controlos fiáveis sobre ativos de TI, OT, IoT, periféricos e dispositivos shadow ou falsificados.

Maior alinhamento com a NIS2: controlos do Artigo 21 relacionados com gestão de ativos, análise de risco, segurança da cadeia de abastecimento, tratamento de incidentes e avaliação de eficácia.

Modelo de responsabilidade partilhada: a Sepio suporta a camada técnica de controlo e a evidência, enquanto os clientes mantêm a responsabilidade pela governação, reporte legal, continuidade do negócio, IAM, MFA, criptografia e programas associados.

Valor para auditoria: os resultados da Sepio podem ser organizados em pacotes recorrentes de evidência para auditoria interna, garantia a clientes e pedidos do regulador.

Como utilizar este guia:

- Utilize a matriz de resumo para compreender rapidamente onde a Sepio tem alinhamento direto, parcial ou de suporte com a NIS2.
- Utilize as secções detalhadas para construir respostas orientadas para clientes, narrativas de auditoria e planos de implementação.
- Utilize a checklist de evidência para definir que relatórios e registos devem ser exportados e conservados de forma recorrente.
- Utilize as notas sobre responsabilidade partilhada para definir expectativas corretas e evitar sobrevalorizar o âmbito da ferramenta.

Contexto de aplicação da Diretiva NIS2:

A NIS2 aplica-se a um vasto conjunto de setores e introduz obrigações para entidades essenciais e importantes. A sua implementação final e os respetivos detalhes de aplicação são definidos na legislação nacional de cada Estado-Membro.

A NIS2 estabelece requisitos em matéria de governação, gestão de riscos de cibersegurança, notificação de incidentes e apresentação de evidências para efeitos de supervisão.

As regras setoriais da UE podem prevalecer sobre obrigações sobrepostas da NIS2 sempre que existam requisitos equivalentes, como sucede com o DORA no caso de muitas entidades financeiras.

A Sepio apoia os seus clientes na conformidade com a NIS2 através de controlos de segurança robustos, gestão de riscos e tratamento de incidentes, devendo ser integrada no enquadramento de controlos já existente do cliente e não tratada como um programa de conformidade autónomo.

A operação da Sepio na UE está fortemente alinhada com os requisitos da NIS2. Antes de finalizarem o seu modelo operacional de conformidade, os clientes devem confirmar o âmbito aplicável, as obrigações de notificação, os locais e as expectativas dos reguladores.

Capacidades base da Sepio para o mapeamento NIS2:

Validação da verdadeira identidade do dispositivo com base no AssetDNA, recorrendo às características da camada física do hardware.

Inventário completo e fiável de ativos de rede, endpoints, periféricos e ambientes ciberfísicos.

Aplicação de controlo de acesso ao hardware baseado em políticas e fluxos de mitigação automatizados.

Monitorização contínua com contexto de localização do dispositivo, histórico de atividade e produção de evidência.

Modelo de visibilidade sem tráfego que se mantém eficaz em ambientes com tráfego encriptado.

Integração com SIEM, SOAR, NAC e ferramentas de ticketing para operacionalizar a resposta e o reporte.

Matriz de resumo de alinhamento entre a NIS2 e a Sepio

Parte A - áreas centrais de controlo técnico

Artigos NIS2	Função da Sepio	Cobertura	Lacuna típica do cliente a preencher
Artigo 20 – Governação	Visibilidade dos ativos para gestão e aplicação de controlos de supervisão	Parcial	Formação do conselho de administração, processos de governação e registos de responsabilidade
Artigo 21(2)(a) – Análise de risco	Base de ativos de confiança e políticas para gestão de risco de hardware	Forte	Processo de gestão de risco empresarial e governação de políticas de segurança
Artigo 21(2)(b) – Gestão de incidentes	Deteta dispositivos não autorizados e suporta fluxos de trabalho de contenção	Forte suporte técnico	Apoio técnico robusto ao processo de resposta a incidentes (IR), incluindo playbooks do CSIRT e fluxos jurídicos e de comunicação
Artigo 21(2)(c) – Continuidade do negócio, backups, recuperação de desastre e gestão de crise	Melhora a análise de impacto e a capacidade de contenção ao nível dos dispositivos	Apoio	Apoio nos processos de recuperação de desastres, gestão de crise e cópias de segurança

Artigos NIS2	Função da Sepio	Cobertura	Lacuna típica do cliente a preencher
Artigo 21(2)(d) – Segurança da cadeia de abastecimento	Valida a identidade dos dispositivos e a aplicação de políticas de acesso ao hardware	Forte	Processos de avaliação de fornecedores e controlos de segurança contratuais
Artigo 21(2)(i) – Gestão de ativos e controlo de acessos	Fornece um inventário de ativos validado ao nível do hardware e políticas de controlo de acesso a nível de dispositivo (permitir/alertar/negar)	Forte	Os processos de IAM da força de trabalho e de RH permanecem sob responsabilidade do cliente

Parte B - comunicação de incidentes, garantia e controlos complementares

Artigos NIS2	Função da Sepio	Cobertura	Lacuna típica do cliente a preencher
Artigo 21(2)(e) – Gestão de vulnerabilidades	Contexto dos ativos e critérios de priorização para correção de vulnerabilidades	Parcial	Processos de gestão de patches, ciclo de vida de desenvolvimento de software e ferramentas de gestão de CVE
Artigo 21(2)(f) – Avaliação da eficácia	Quantificação de violações de políticas, indicadores de risco e resultados de mitigação, para avaliação da eficácia e suporte a auditorias	Forte suporte	Programa formal de KPI e auditorias
Artigo 21(2)(g)(h)(j) – Formação, criptografia e autenticação multifator	Complementa a validação de dispositivos e a aplicação de políticas de controlo de acesso	Suporte	Sistemas de gestão de aprendizagem, gestão de identidades e acessos, autenticação multifator, infraestrutura de chave pública e comunicações seguras
Artigo 23 – Notificação de incidentes	Deteção mais rápida, triagem e evidência para cumprimento dos prazos de notificação	Forte suporte	Processo de reporte ao CSIRT ou à autoridade reguladora
Artigos 32 to 34 - Supervision and fines	Evidência pronta para auditoria no âmbito da implementação e da due diligence	Forte evidence layer	Governação do programa e interação com o regulador

Mapeamento detalhado de controlos

Artigo 20 - Governação e responsabilidade da gestão

Nível de cobertura: Parcial

Expectativa da NIS2

Espera-se que os órgãos de gestão aprovem e supervisionem as medidas de gestão do risco de cibersegurança e assegurem formação e sensibilização adequadas para a gestão.

Como a Sepio apoia

- Fornece uma visão fiável dos ativos conectados e da identidade dos dispositivos, permitindo compreender a exposição ciberfísica da rede.
- Fornece outputs de políticas de acesso, alertas de risco e evidências de mitigação para revisão do conselho de administração e da direção executiva.
- Contribui para a demonstração de devida diligência através de melhorias mensuráveis na visibilidade e no controlo do risco de hardware.

Responsabilidades do cliente e do ecossistema

- O cliente deve manter estruturas de governação, fluxos de aprovação e registos de responsabilização da gestão.
- O cliente deve executar programas de formação e sensibilização da gestão e manter comprovativos de participação e conclusão.
- As equipas jurídicas e de conformidade devem alinhar as políticas com a implementação nacional da NIS2 em cada jurisdição.

Evidências recomendadas para auditores e clientes

- Relatórios executivos que demonstram a postura dos ativos e as tendências de aplicação de controlos.
- Documentos de políticas de acesso a hardware aprovadas e registos de alterações.
- Atas de revisão da gestão e registos de aprovação.
- Pacotes trimestrais de revisão de conformidade com referência aos outputs da Sepio.

Artigo 21(2)(a) - Análise de risco e políticas de segurança

Nível de cobertura: Forte

Expectativa da NIS2

As entidades devem definir e manter políticas de análise de risco e segurança dos sistemas de informação, com controlos que reflitam a exposição e o contexto operacional da organização.

Como a Sepio apoia

- Com base em dados físicos de hardware, constrói uma camada fiável de ativos, incluindo dispositivos não geridos ou shadow, que ferramentas apenas de software podem não identificar.
- Suporta decisões de política de acessos com base no tipo de dispositivo, identidade, localização, interface e contexto de risco observado.
- Melhora a qualidade da análise de risco com dados fiáveis sobre a conectividade de hardware.

Responsabilidades do cliente e do ecossistema

- O cliente deve manter a metodologia de risco corporativo, os critérios de aceitação de risco e a governação de aprovação de políticas.
- O cliente deve integrar os outputs da Sepio em indicadores de risco mais amplos e em frameworks de controlo.
- O cliente deve definir exceções de política e controlos compensatórios para dispositivos não normalizados.

Evidências recomendadas para auditores e clientes.

- Registos de alertas e cronologias de incidentes da Sepio e de ferramentas integradas.
- Relatórios de verificação de identidade de dispositivos com AssetDNA.
- Playbooks de resposta a incidentes que referenciam dados e alertas da Sepio.
- Registo de exceções e isenções para desvios de políticas de hardware.

Artigo 21(2)(b) - Tratamento de incidentes

Nível de cobertura: Forte suporte técnico

Expectativa da NIS2

As entidades devem manter capacidades de gestão de incidentes, incluindo deteção, triagem, contenção, remediação e coordenação.

Como a Sepio apoia

- Deteta atividades de hardware não autorizadas, fraudulentas, falsificadas ou não geridas, bem como violações de políticas.
- Suporta fluxos de trabalho automatizados de contenção, isolamento, bloqueio e escalamento através da aplicação de políticas e integrações.
- Fornece o histórico e o contexto do dispositivo, o que melhora a triagem de incidentes e os cronogramas forenses.

Responsabilidades do cliente e do ecossistema

- O cliente deve operar um processo formal de resposta a incidentes, um modelo de gravidade e uma autoridade de decisão.
- O cliente deve manter procedimentos legais, de comunicação e de notificação.
- As equipas de resposta a incidentes devem documentar a causa raiz, o impacto e as ações de recuperação em toda a stack tecnológica.

Evidências recomendadas para auditores e clientes.

- Registos de alertas e cronologias de incidentes da Sepio e de ferramentas integradas.
- Histórico de ações de mitigação, incluindo bloqueios, isolamentos e escalonamentos.
- Playbooks de resposta a incidentes que referenciam dados e alertas da Sepio.
- Relatórios pós-incidente com evidências de hardware e dispositivo anexadas.

Artigo 21(2)(c) - Continuidade do negócio, backup, recuperação de desastre e gestão de crise

Nível de cobertura: suporte

Expectativa da NIS2

As entidades devem manter medidas de resiliência como backups, planos de recuperação de desastre, procedimentos de crise e capacidades de continuidade.

Como a Sepio apoia

- Melhora a consciência situacional durante incidentes, identificando rapidamente dispositivos afetados ou não fiáveis.
- Auxilia no confinamento de hardware suspeito para reduzir a disseminação e o impacto operacional.
- Fornece evidências ao nível do dispositivo que podem melhorar a análise de impacto e a priorização da recuperação.

Responsabilidades do cliente e do ecossistema

- O cliente deve manter plataformas de cópia de segurança, testes de restauro e manuais de recuperação de desastres.
- O cliente deve definir os procedimentos de comunicação de crise, continuidade de negócio e escalamento para a administração.
- As equipas de infraestruturas devem executar a recuperação e validação do sistema fora da Sepio.

Evidências recomendadas para auditores e clientes

- Manuais de resposta a crises que incluem etapas de quarentena e validação de dispositivos.
- Relatórios de testes de recuperação que fazem referência aos outputs de descoberta e contenção da Sepio.
- Planos de continuidade mapeados para locais críticos e grupos de ativos.
- Lições aprendidas após o evento, incluindo descobertas ao nível do hardware.

Artigo 21(2)(d) - Segurança da cadeia de abastecimento

Nível de cobertura: Forte em termos de hardware e de confiança nos dispositivos

Expectativa da NIS2

As entidades devem abordar os riscos cibernéticos relacionados com a cadeia de abastecimento e com os fornecedores, incluindo os riscos provenientes de fornecedores diretos, prestadores de serviços e preocupações com a fiabilidade dos produtos.

Como a Sepio apoia

- Valida o que um dispositivo realmente é, e não apenas o que afirma ser na rede.
- Deteta hardware e periféricos falsificados, ocultos ou não aprovados que podem indicar um comprometimento da cadeia de abastecimento ou uma substituição não autorizada.
- Permite a aplicação de políticas com base no fabricante, modelo, tipo de dispositivo e localização, reduzindo a exposição a hardware não confiável.

Responsabilidades do cliente e do ecossistema

- O cliente deve executar processos de due diligence de fornecedores, contratação e gestão de riscos de terceiros.
- As equipas de compras e jurídicas devem definir as cláusulas de segurança do fornecedor e os requisitos de comprovação.
- Responsabilização de ativos: atribuir responsabilidade pelos ativos e gerir o respetivo ciclo de vida, integrando ferramentas de descoberta técnica no framework de controlo.

Evidências recomendadas para auditores e clientes

- Listas de políticas de dispositivos e fornecedores aprovados.
- Relatórios de deteção de hardware não autorizado, falsificado ou não conforme.
- Aprovações de exceção para dispositivos de fornecedores temporários ou de alto risco.
- Registos de garantia do fornecedor com referências cruzadas aos controlos de política de dispositivos.

Artigo 21(2)(i) - Gestão de ativos e controlo de acesso

Nível de cobertura: Forte para ativos físicos

Expectativa da NIS2

As entidades devem manter a segurança dos recursos humanos, políticas de controlo de acesso e gestão de ativos. Esta cláusula é breve, mas intencionalmente ampla, e constitui uma parte significativa do Artigo 21.º.

Como a Sepio apoia

- Inventário de ativos verificado: a Sepio fornece um inventário de ativos validado ao nível do hardware de todos os dispositivos conectados, incluindo dispositivos não geridos e falsificados.
- Controlo de acesso ao hardware: A Sepio aplica políticas de acesso ao nível do dispositivo (permitir/alertar/bloquear) para evitar ligações de hardware não autorizadas ou de alto risco.
- Evidências de aplicação de políticas: A Sepio gera registos contínuos e registos de aplicação para comprovar a governação eficaz dos ativos e o controlo de acesso.

Responsabilidades do cliente e do ecossistema

- Segurança de RH: Gerir a integração de novos colaboradores, mudanças de funções, despedimento e revisões periódicas de acesso.
- Governação de acesso: Definir e aplicar políticas de acesso de utilizadores e administradores (IAM, MFA, privilégio mínimo, exceções).
- Responsabilidade pelos ativos: Atribuir a propriedade dos ativos e a governação do ciclo de vida, integrando ferramentas de descoberta técnica na estrutura de controlo.

Evidências recomendadas para auditores e clientes

- Inventário de ativos: Visibilidade validada por hardware de todos os ativos ligados, incluindo dispositivos não geridos e falsificados, bem como novos dispositivos adicionados em qualquer intervalo (diário, semanal, etc.).
- Controlo ao nível do dispositivo: Controlo baseado em políticas (permitir/alertar/bloquear) das ligações dos dispositivos no ponto de acesso.
- Evidências prontas para auditoria: Registos e relatórios contínuos que mostram a presença de ativos, a aplicação de políticas e os resultados do controlo de acesso.

Artigo 21(2)(e) - Aquisição, desenvolvimento, manutenção e tratamento de vulnerabilidades

Nível de cobertura: Parcial

Expectativa da NIS2

As entidades devem gerir a cibersegurança nas fases de aquisição, desenvolvimento e manutenção, incluindo os processos de tratamento e divulgação de vulnerabilidades.

Como a Sepio apoia

- Fornece contexto de hardware e ativos que melhora a priorização da correção e a tomada de decisões operacionais.
- Identifica dispositivos de risco ou não geridos e pode desencadear ações de workflow através de integrações.
- Ajuda as equipas de segurança a priorizar ações de correção (patching) e resposta com base na presença verificada dos dispositivos e na respetiva exposição.

Responsabilidades do cliente e do ecossistema

- O cliente deve assegurar a gestão de patching, a análise de vulnerabilidades e a governação da remediação.
- As equipas de desenvolvimento devem manter processos seguros de SDLC (Software Development Life Cycle) e de divulgação de vulnerabilidades.
- As equipas de GRC (Governação, Risco e Conformidade) devem monitorizar os prazos de remediação, as exceções e os controlos compensatórios.

Evidências recomendadas para auditores e clientes

- Relatórios de exposição de ativos utilizados para o rastreio de vulnerabilidades.
- Fluxos de trabalho integrados com tickets e registos de ações corretivas.
- Registos de aplicação de políticas para dispositivos não atualizados ou com acesso restrito.
- Documentação de exceção e aceitação de risco ligada ao inventário de dispositivos.

Artigo 21(2)(f) - Avaliação da eficácia das medidas de cibersegurança

Nível de cobertura: Forte suporte

Expectativa da NIS2

As entidades devem avaliar a eficácia das medidas de gestão de riscos de cibersegurança através de políticas, procedimentos e análises baseadas em evidências.

Como a Sepio apoia

- Fornece resultados mensuráveis, como dispositivos não autorizados detetados, violações de políticas e ações de mitigação executadas.
- Suporta a monitorização contínua e a evidência histórica para análise de tendências e validação de controlos.
- Ajuda a demonstrar que os controlos de confiança de hardware estão ativos, aplicados e a produzir resultados.
- Gera indicações mensuráveis baseadas no risco para todos os ativos físicos.

Responsabilidades do cliente e do ecossistema

- O cliente deve definir os KPI, a frequência dos testes, o âmbito da auditoria e a responsabilidade pela revisão.
- O cliente deve realizar testes periódicos de controlos, simulações de incidentes e exercícios de resposta.
- As equipas de auditoria e compliance devem consolidar as evidências da Sepio e de outros sistemas num pacote de avaliação formal.

Evidências recomendadas para auditores e clientes

- Painéis de KPIs mensais e trimestrais.
- Análise de tendências de violações de políticas e tempos de resposta.
- Registos de auditoria de ações de fiscalização e alterações de políticas.
- Atas de revisão da eficácia dos controlos e planos de ação corretiva.
- Relatórios flexíveis baseados em níveis de risco, tipos de ativos, localização e proximidade dos ativos críticos da organização.

Artigo 21(2)(g), (h), and (j) - Higiene cibernética, formação, MFA e criptografia

Nível de cobertura: De suporte

Expectativa da NIS2

A NIS2 também exige práticas básicas de higiene cibernética e formação, políticas de criptografia e encriptação, bem como práticas seguras de autenticação e comunicações.

Como a Sepio apoia

- Reforça estes controlos de forma indireta, promovendo a utilização de hardware de confiança e reduzindo as vias de acesso a dispositivos não autorizados.
- Fornece exemplos práticos de incidentes e o estado da aplicação de políticas que podem ser utilizadas em programas de sensibilização e formação.
- Complementa os controlos de IAM, MFA e de comunicações seguras, através da validação do componente de confiança ao nível do dispositivo.

Responsabilidades do cliente e do ecossistema

- O cliente deve executar programas de formação e sensibilização e manter registos de conclusão.
- O cliente deve implementar o IAM, MFA, PKI, encriptação e controlos de comunicação segura.
- As equipas de arquitetura e de segurança devem definir claramente os pontos de integração entre a Sepio, o NAC, o IAM e os controlos de segurança de rede.

Evidências recomendadas para auditores e clientes

- Conteúdos de formação que abordam a validação dos dispositivos a cenários de políticas de hardware.
- Diagramas de arquitetura que mostram a integração da Sepio com IAM, NAC e SIEM.
- Relatórios de políticas de dispositivos que demonstram a aplicação do princípio do menor privilégio de acesso.
- Mapeamento de controlos que documenta as fronteiras de âmbito entre a Sepio e as ferramentas de IAM e criptografia.

Artigo 23 - Reporte de incidentes significativos

Nível de cobertura: Forte suporte (não inclui o processo de submissão).

Expectativa da NIS2

As entidades devem comunicar os incidentes significativos de acordo com as normas nacionais NIS2, que normalmente exigem um alerta prévio no prazo de 24 horas, uma notificação formal no prazo de 72 horas e o cumprimento dos prazos para o relatório final.

Como a Sepio apoia

- Acelera a deteção e triagem de eventos relacionados com hardware através da verificação da identidade do dispositivo e da monitorização contínua.
- Fornece o contexto exato do dispositivo, como o tipo, a localização e o estado da aplicação das políticas, para garantir a precisão dos relatórios.
- Recolhe evidências de mitigação e histórico que suportam as narrativas de incidentes e a preparação de pacotes de reporte destinados aos reguladores.

Responsabilidades do cliente e do ecossistema

- O cliente deve definir os limites para os incidentes comunicáveis e alinhá-los com os requisitos nacionais do CSIRT ou das entidades reguladoras.
- O cliente deve manter os fluxos de trabalho de submissão, revisão jurídica e aprovações de comunicação.
- Os responsáveis pelos incidentes devem consolidar os dados da Sepio com análises forenses, de rede e de impacto no negócio.

Evidências recomendadas para auditores e clientes

- Registo da data e hora da deteção e cronologia do evento.
- Os dispositivos afetados e detalhes de identidade verificados.
- As ações de mitigação tomadas e estado atual.
- Registos de aprovação interdepartamental e pacote final de relatório de incidente.

Artigo s 32 to 34 - Supervisão, auditorias, fiscalização e coimas

Nível de cobertura: Forte enquanto camada de evidência

Expectativa da NIS2

A NIS2 atribui às autoridades competências de supervisão, incluindo a possibilidade de solicitar evidências, auditorias e prova de implementação, prevendo igualmente coimas significativas em caso de incumprimento.

Como a Sepio apoia

- Produz evidência pronta para auditoria relativa ao inventário de ativos, à aplicação de políticas, às ações de resposta a incidentes e aos resultados de monitorização.
- Suporta a demonstração de evidência através da operação contínua dos controlos e da mitigação mensurável dos riscos.
- Permite a geração de pacotes de evidência para auditoria interna, garantia aos clientes e resposta a pedidos dos reguladores.

Responsabilidades do cliente e do ecossistema

- O cliente continua responsável pela conformidade legal, pelas respostas às autoridades e pela gestão formal das auditorias.
- As equipas de compliance devem organizar as evidências da Sepio em articulação com os processos de governação, IAM, continuidade de negócio e recuperação de desastre (BC/DR) e reporte.
- Os clientes devem designar um responsável pelas exportações recorrentes de provas e pelas revisões de prontidão regulamentar.

Evidências recomendadas para auditores e clientes

- Pacote de provas recorrentes, incluindo a linha de base do inventário, a validação do AssetDNA, o catálogo de políticas e os registos de aplicação.
- Inteligência de vulnerabilidades, relatórios com reconhecimento de localização e registos históricos de atividades do dispositivo.
- Evidências de integração de SIEM, SOAR, NAC e fluxos de trabalho de emissão de tickets.
- Modelos de resposta a auditorias e responsáveis nomeados para pedidos de entidades reguladoras.

Roadmap de implementação para o cliente

O guia abaixo foi concebido para apoiar discussões de planeamento com o cliente, posicionando a Sepio como um controlo fundamental. Destaca igualmente as responsabilidades partilhadas necessárias para garantir a prontidão face à NIS2.

Fase	Objetivo principal	Ações da Sepio	Ações do cliente	Resultados
1. Âmbito e Linha de Base	Definir a aplicabilidade e estabelecer uma linha de base fiável dos dispositivos (“device truth”)	Descobrir os ativos, validar a cobertura e consolidar o inventário de referência, assegurando visibilidade através do AssetDNA	Confirmar o âmbito de aplicação, as obrigações setoriais aplicáveis, os locais prioritários e o modelo de controlos-alvo	Memorando de definição do âmbito, inventário de referência e avaliação inicial de riscos
2. Desenho de política	Traduzir os objetivos da política em controlos de hardware aplicáveis	Criar conjuntos de políticas para dispositivos aprovados, deteção de dispositivos não autorizados e restrições baseadas na localização ou função	Aprovar os responsáveis pelas políticas, as exceções, o processo de alteração e os limites de aplicação	Catálogo de políticas, processo de exceções, plano piloto
3. Integração e resposta a incidentes	Operacionalizar a deteção e a mitigação	Integrar com SIEM, SOAR, NAC e sistemas de ticketing, ativando ações automatizadas e o registo de evidências	Atualizar os manuais de resposta a incidentes e validar os canais legais e de comunicação	Fluxos de trabalho integrados e manuais de procedimentos testados
4. Preparação para auditoria e elaboração de relatórios	Criar uma capacidade recorrente de geração de evidência e de reporte	Agendar exportações e painéis de controlo para inventário, políticas, incidentes e aplicação de medidas de controlo	Definir modelos de relatório, frequência de revisão e responsáveis pelas evidências	Pacote trimestral de evidência e revisão de preparação

Pacote de Evidência Recomendado da Sepio para Programas NIS2

Os clientes devem elaborar um pacote de provas recorrente mensalmente ou trimestralmente. O objetivo é demonstrar que os controlos não só estão definidos, mas em funcionamento e a produzir resultados mensuráveis.

- **Inventário de Ativos de Rede -** inventário completo por local, segmento e classe de ativos críticos, incluindo ativos não geridos e ativos ocultos.
- **Evidência de AssetDNA e validação da identidade dos dispositivos -** Registos de deteções de dispositivos desconhecidos, falsificados ou que violem as políticas e os seus respetivos destinos.
- **Catálogo de políticas e respetivas aprovações -** incluindo versões das políticas, responsáveis, modo de aplicação e registos de exceção.
- **Registos de aplicação e mitigação de políticas** - alertas, ações de bloqueio ou isolamento, escalonamentos e resultados do fluxo de trabalho.
- **Relatórios de vulnerabilidades e contextualização da exposição -** priorização de grupos de dispositivos e os resultados de apoio à correção.
- **Relatórios de localização e histórico de ativos -** incluindo o contexto de localização dos dispositivos e a atividade histórica para suporte a investigações.
- **Evidências de integração -** registos de SIEM, SOAR, NAC e de tickets que comprovam a execução do workflow end-to-end.
- **Relatório de eficácia dos controlos -** incluindo tendências de KPI, resultados de testes de controlos e decisões de revisão pela gestão.

Modelo de responsabilidade partilhada

A Sepio constitui uma camada de controlo crítica para a confiança nos dispositivos e a mitigação do risco de hardware; no entanto, a conformidade com a NIS2 permanece um programa abrangente que envolve pessoas, processos e múltiplas tecnologias.

Responsabilidades da Sepio	Responsabilidade do cliente	Resultados partilhados
Descoberta de dispositivos e validação de identidade	Governação, aprovação de políticas e responsabilidade legal	Controlos de gestão de riscos fiáveis e auditáveis
Aplicação de políticas de hardware e ativação de mecanismos de mitigação de risco	Decisões de resposta a incidentes e submissão de relatórios às entidades reguladoras	Contenção mais célere e evidência de reporte mais robusta e verificável
Monitorização contínua e geração de evidências técnicas	Testes de controlo, gestão de auditorias e retenção de evidência	Devida diligência e eficácia comprovada
Integração com ferramentas do ecossistema	Modelo operacional, dotação de pessoal adequada e coordenação eficaz entre equipas	Preparação para a NIS2 operacionalizada ao longo de toda a stack tecnológica

Nota setorial para entidades financeiras

Para muitas entidades financeiras, o DORA pode definir as principais obrigações de cibersegurança e de reporte de incidentes onde estas se sobrepõem à NIS2. Nestes casos, posicione a Sepio como alinhada com a NIS2 e compatível com o DORA, e confirme os requisitos aplicáveis através das orientações nacionais de implementação e supervisão aplicáveis.

- ✔ Utilizar este guia como referência para o alinhamento de controlos de confiança em hardware e de visibilidade de ativos.
- ✔ Validar as principais obrigações de reporte e de supervisão aplicáveis ao abrigo do regime setorial relevante.
- ✔ Sempre que possível, manter um modelo único de evidência, assegurando que os resultados da Sepio suportam simultaneamente os requisitos regulamentares e as necessidades de garantia ao cliente.

Posicionamento sugerido para apresentação ao cliente

A Sepio ajuda as organizações a operacionalizar os principais requisitos de controlo da NIS2, fornecendo identidade de dispositivos verificada através do AssetDNA, visibilidade completa dos ativos, aplicação de políticas de acesso a hardware e fluxos de mitigação automatizados. É particularmente eficaz na deteção de dispositivos não geridos, não autorizados e falsificados, que as soluções tradicionais baseadas apenas em software frequentemente não conseguem identificar. A Sepio fornece ainda a evidência necessária para suportar a gestão de incidentes, a preparação para auditorias e o reporte orientado a reguladores.

Próximos passos para projetos com clientes

1

Executar uma avaliação de descoberta de curta duração para obter visibilidade dos ativos e identificar dispositivos não geridos ou não fiáveis.

2

Priorizar um ou dois casos de uso de política de maior impacto, como bloquear dispositivos USB não aprovados ou aplicar a política para adaptadores de rede aprovados.

3

Integrar os alertas da Sepio no workflow existente de tratamento de incidentes e testar um cenário de reporte.

4

Definir o pacote recorrente de evidência NIS2 e atribuir responsáveis por exportação, revisão e retenção.

5

Rever o mapeamento final de controlos face à implementação nacional da NIS2, com o apoio das equipas jurídica e de compliance.

Nota importante: Este guia explica como a Sepio suporta os objetivos de controlo da NIS2. Trata-se de um documento de alinhamento técnico e operacional, não constituindo aconselhamento jurídico. A NIS2 é implementada através de legislação nacional, pelo que os clientes devem confirmar as obrigações finais com assessoria jurídica e de compliance em cada país de operação. A Sepio é aqui posicionada como uma camada de controlo técnico essencial para confiança em hardware, visibilidade e aplicação de políticas, no âmbito de um programa de conformidade mais amplo.

Isenção de responsabilidade: Este documento destina-se ao planeamento do alinhamento da conformidade e à comunicação com o cliente Não constitui aconselhamento jurídico.