ASSA ABLOY

Whitepaper

Requisitos NIS2 e orientações para proteção física e controlo de acessos

Reforçar a resiliência ciberfísica com soluções de acesso digital e gestão remota

Experience a safer
and more open world

Neste whitepaper, vai aprender sobre:

A partir de 17 de outubro de 2024, o cumprimento da Diretiva NIS2 tornou-se obrigatório, exigindo que todos os Estados-Membros da UE transpusessem a diretiva para a legislação nacional. Este whitepaper baseia-se no estado atual da Diretiva NIS2 (UE) 2022/2555 e na sua implementação nos Estados-Membros da UE até meados de 2025. Embora vários países já tenham aprovado legislação nacional, outros ainda se encontram em fase de transposição, podendo os prazos e requisitos sofrer alterações. Os leitores devem ter em conta que o enquadramento legal e regulamentar pode evoluir e são aconselhados a consultar fontes oficiais atualizadas ou apoio jurídico especializado para obter informação mais recente. Este whitepaper tem fins exclusivamente informativos e não constitui aconselhamento jurídico.

A Diretiva NIS2

Novas exigências e desafios emergentes

Esta legislação europeia de cibersegurança substitui a diretiva original NIS relativa à Segurança das Redes e da Informação, de 2016. A atualização legislativa reforça os requisitos mínimos de segurança informática para infraestruturas críticas e alarga o âmbito a setores adicionais. Isto significa que, com a transposição da NIS2 para as legislações nacionais em toda a Europa, muito mais áreas e empresas serão abrangidas do que anteriormente.

É fundamental compreender que a nova diretiva de cibersegurança exige uma abordagem abrangente à gestão de riscos. Isto significa que os responsáveis devem não só implementar medidas de segurança digital, mas também adotar precauções para proteger fisicamente as suas infraestruturas.

Estes são os temas abordados no restante deste whitepaper:

- Que empresas estão sujeitas à NIS2
- Quais os requisitos específicos envolvidos
- Como as organizações podem reforçar a resiliência ciberfísica com soluções de acesso digital

A NIS2 vai muito além do simples cumprimento de requisitos de cibersegurança. Exige que a segurança física trabalhe em conjunto com as proteções digitais, inaugurando uma nova era de normas de **resiliência ciberfísica**.

Quem é abrangido pela NIS2?

A aplicação da Diretiva NIS2 a uma empresa depende, antes de mais, da sua inclusão em um dos 18 setores definidos. Estes setores estão distribuídos por dois anexos e divididos entre: “Setores de elevada criticidade” e “Outros setores críticos” A classificação segue o sistema europeu de setores económicos NACE.

Além das áreas de atividade, a dimensão e o desempenho económico de uma organização também são determinantes para a sua categorização. Com base nestes fatores, a NIS2 distingue entre “Entidades essenciais” e “Entidades importantes”.

Responsabilidade legal e prestação de contas ao nível da gestão

De acordo com a Diretiva (UE) 2022/2555 (NIS2), as entidades podem enfrentar coimas até 10 milhões de euros, ou 2% do volume de negócios anual global, em caso de incumprimento. Os Estados-Membros devem garantir que os órgãos de gestão podem ser responsabilizados por violações resultantes de negligência grave ou falta de supervisão. As autoridades de supervisão podem ainda impor suspensões temporárias que impedem membros da gestão de exercer funções de liderança.

Pode consultar o texto legal completo no *EUR-Lex* [1]

1 *https://www.hidglobal.com/resource-center/reports/state-of-security-and-identity-2025*

Quem é abrangido pela NIS2?

ANEXO I — Setores e subsetores de elevada criticidade

Energia Abastecimento de eletricidade, aquecimento/ arrefecimento urbano, combustíveis/ petróleo, gás

Transportes / Tráfego Transporte aéreo, transporte ferroviário, transporte marítimo, transporte rodoviário

Finanças / Seguros Bancos, infraestruturas dos mercados financeiros

Saúde Serviços de saúde, laboratórios de referência, I&D, indústria farmacêutica (NACE C, Divisão 21), dispositivos médicos

Água / Águas residuais Abastecimento de água e gestão de águas residuais

Gestão de Serviços CT (apenas B2B) Prestadores de serviços geridos e prestadores de serviços geridos de segurança

Espaço Infraestruturas terrestres

Casos especiais* Prestadores qualificados de serviços de confiança (qTSPs), registos de domínios de topo (TLD), fornecedores de serviços DNS, operadores de telecomunicações, instalações críticas, organismos da administração central; prestadores de serviços de confiança (TSPs).

Entidade essencial
- Tem pelo menos 250 trabalhadores; ou
- Gera mais de 50 milhões de euros em volume de negócios anual; e
- Tem um total de balanço superior a 43 milhões de euros

Entidade essencial*
A NIS2 aplica-se a todas as empresas destes setores que excedam 10 milhões de euros de volume de negócios anual, independentemente da sua dimensão.*

ANEXO II — Outros setores críticos e subsetores

Transportes / Tráfego Serviços postais e de correio

Químicos Fabrico, comércio e produção

Investigação Instituições de investigação

Setor da indústria transformadora Equipamentos médicos / diagnóstico, TI, eletrónica, ótica (NACE C, Divisões 26 e 27)

Engenharia mecânica (NACE C 28) Automóvel / Componentes (NACE C 29) Fabricação de veículos (NACE C 30)

Serviços digitais Marketplaces, motores de busca e redes sociais

Alimentação Comércio por grosso, produção e transformação

Gestão de resíduos Recolha e eliminação de resíduos

Entidade importante
- Tem pelo menos 50 trabalhadores; ou
- Gera mais de 10 milhões de euros em volume de negócios anual e em total de balanço

* Para além disso, empresas mais pequenas também podem ser abrangidas pela NIS2 .Isto aplica-se quando a sua falha teria consequências significativas para a economia ou para os serviços públicos. Isto inclui, por exemplo, determinados serviços digitais regulados pelo Regulamento eIDAS (Regulamento da UE n.º 910/2014 relativo à Identificação Eletrónica, Autenticação e Serviços de Confiança). No entanto, as microempresas — aquelas com menos de nove trabalhadores e um volume de negócios anual inferior a 2 milhões de euros — não são abrangidas.

A NIS2 e a importância da segurança e proteção física

Em princípio, as entidades essenciais e importantes devem, de acordo com o Artigo 21 da Diretiva NIS2, "adotar medidas técnicas, operacionais e organizacionais adequadas e proporcionais para gerir os riscos para a segurança das redes e dos sistemas de informação [...] e para prevenir ou minimizar o impacto de incidentes de segurança nos destinatários dos seus serviços e noutros serviços." Estas medidas devem ter em conta o estado da arte e o cenário específico de ameaças de cada organização.

Um ponto fundamental é que estas medidas de proteção devem seguir uma abordagem abrangente de gestão de riscos. Isto significa não apenas defender contra ameaças digitais aos sistemas de rede e informação, mas também proteger fisicamente o ambiente onde esses sistemas operam, reduzindo o risco de incidentes de segurança que possam comprometer a continuidade do serviço.

O facto de a nova diretiva enfatizar tão claramente este aspeto não é uma coincidência.

A Agência da União Europeia para a Cibersegurança (ENISA) destaca explicitamente, numa recente avaliação de ameaças [2], o aumento dos chamados ataques ciberfísicos.

À medida que os produtos se tornam cada vez mais interligados através da Internet das Coisas (IoT), as vulnerabilidades existentes oferecem potenciais pontos de entrada — por exemplo, para obter acesso a áreas de alta segurança que estão fisicamente protegidas.

Apesar de muitos organismos já terem planos híbridos que combinam segurança cibernética e física, a ENISA continua a considerar o acesso físico como a "maior porta traseira", cuja importância é frequentemente subestimada.

Neste contexto, são particularmente vulneráveis os terminais de acesso público, unidades de armazenamento ou monitores, que se podem tornar alvos fáceis de vandalismo ou sabotagem, por exemplo através de dispositivos USB maliciosos.

O acesso físico é considerado a maior porta de entrada para cibercriminosos. **Poderá a sua organização estar em risco?**

2 https://www.hidglobal.com/resource-center/reports/state-of-security-and-identity-2025

Resiliência ciberfísica

Proteger a TI e a segurança dos dados contra ciberataques

Proteger TI, dados e infraestruturas através de medidas físicas

Proteção física abrangente da sua organização e dos seus dados

Quer na indústria, na administração pública ou na área da saúde, os centros de dados modernos formam o coração de muitas organizações, funcionando como polos centrais de controlo e armazenamento para a troca eletrónica de informação. Garantir uma proteção eficaz dos ativos físicos e digitais concentrados nestes locais é essencial para manter funções críticas da organização e preservar a reputação empresarial.

Os padrões e as "boas práticas" já estabelecidos para proteger estas áreas sensíveis constituem uma base sólida para a implementação de medidas adequadas em toda a infraestrutura operacional, tal como previsto pela Diretiva NIS2.

Como ponto de referência inicial, recomenda-se a série de normas europeias EN 50600 ("Instalações e Infraestruturas de Centros de Dados")[3], que descreve um modelo de segurança em camadas baseado no "princípio da casca de cebola". Neste modelo, diferentes classes de segurança são construídas em camadas sucessivas, aumentando o nível de proteção do exterior para o interior.

Construir resiliência ciberfísica: o modelo de segurança em camadas alinhado com a NIS2

Classe de Proteção 4
Acesso estritamente regulado, áreas centrais críticas Servidor / TI, rede com bastidores e armários de servidores

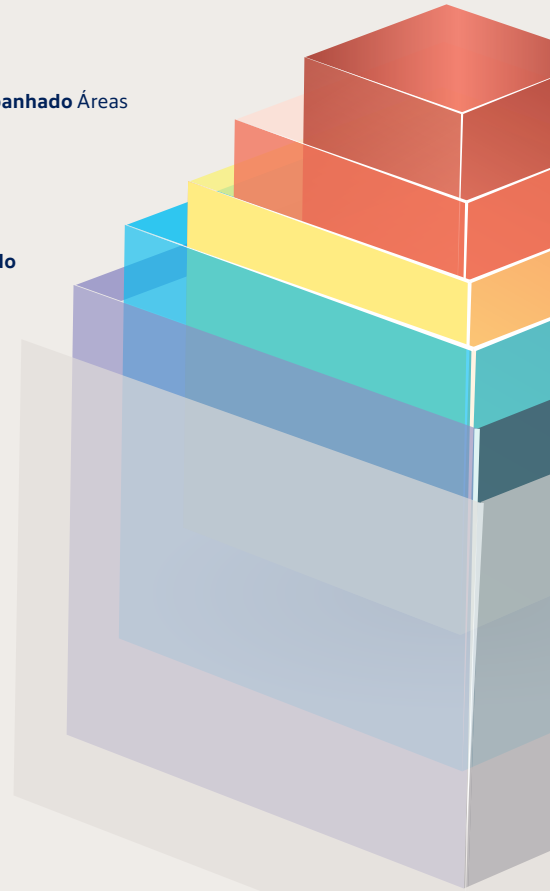
Classe de Proteção 3
Acesso restrito + acesso acompanhado Áreas técnicas com portas e armários

Classe de Proteção 2
Acesso regulado + acesso acompanhado Escritórios e áreas especializadas com portas e armários

Classe de Proteção 1
Acesso público restrito Entrada do edifício e envolvente exterior com portas / zonas periféricas com vedação

Classe de Proteção 0
Áreas abertas, semipúblicas

Classe de Proteção -1
Espaço público



3 https://landingpage.bsigroup.com/LandingPage/Series?UPI=BS%20EN%2050600

Impulsionar a gestão de risco: envolver todos e passar à ação

No mínimo, devem ser cumpridos os seguintes requisitos:

- Conceitos bem desenvolvidos para análise de risco e segurança de sistemas de TI, bem como para a gestão de incidentes de segurança
- Medidas para garantir a continuidade do negócio (Business Continuity Management), incluindo gestão de crises e procedimentos de backup para recuperação de dados
- Segurança da cadeia de abastecimento (gestão de parceiros de negócio e prestadores de serviços, medidas de segurança durante a aquisição e desenvolvimento de sistemas de informação)
- Segurança na aquisição, desenvolvimento e manutenção de sistemas de TI e de rede, incluindo a gestão de vulnerabilidades
- Diretrizes para medir a cibersegurança e as medidas de mitigação de risco
- Formação em segurança de TI e práticas básicas de higiene digital (por exemplo, princípios de zero trust, atualizações de software, configuração de dispositivos, segmentação de rede, gestão de identidades e acessos, ou sensibilização dos utilizadores[4])
- Criptografia e encriptação de dados
- Autenticação e comunicação seguras
- Manutenção da funcionalidade do sistema durante falhas de energia, se for eletrónico e ligado por cabos

Segurança do pessoal, incluindo **conceitos de controlo de acesso físico** e gestão de instalações (ISMS / Sistema de Gestão de Segurança da Informação)

4 *https://www.nis-2-directive.com/NIS_2_Directive_Preamble_81_to_90.html*

Identificação e eliminação de potenciais vulnerabilidades no acesso físico

Quanto mais cedo as organizações começarem a se preparar para a NIS2, melhor – e **as medidas para a proteção física das instalações desempenham um papel central** nesse processo. Durante as suas avaliações, os responsáveis pela segurança devem avaliar minuciosamente as medidas de segurança existentes, incluindo **sistemas de controlo de acesso e bloqueio,** para determinar a sua eficácia a longo prazo.

Sistemas mecânicos de fecho mais antigos podem representar riscos de responsabilidade significativos para os operadores, especialmente se a proteção de patente tiver expirado. Nesses casos, os serralheiros deixam de ser obrigados a contactar o fabricante e podem ser feitas cópias de chaves sem qualquer verificação. Isto representa um risco de segurança sério. As empresas podem ter de suportar elas próprias os custos de potenciais interrupções de serviço se não conseguirem demonstrar que implementaram medidas de proteção adequadas.

A experiência mostra que, quanto mais antigos são estes sistemas de fecho, mais difícil se torna controlar o número de chaves em circulação e responder rapidamente a perdas de chaves. A checklist ao lado pode ajudar uma organização a determinar se, e onde, é necessária uma intervenção urgente.

As empresas **devem** demonstrar que têm medidas adequadas de segurança física implementadas.

Checklist: Quão preparado para o futuro está o meu acesso físico?

- Existe um conceito de segurança bem desenvolvido para o acesso físico?
- Os eventos de acesso são rastreáveis e documentados?
- Quão rapidamente é possível responder à perda de chaves/credenciais?
- Existem chaves/credenciais não autorizadas potencialmente em circulação?
- Quão abrangente é o sistema de gestão de chaves/credenciais?
- O hardware está atualizado e é possível proteger pontos de acesso críticos para além das portas (por exemplo, armários, racks de servidores, portões, etc.)?
- A operação contínua está garantida em caso de falha de energia (apagão)?
- Se estiver a ser utilizado um sistema mecânico de fecho, este possui proteção de patente válida?

Como as soluções de acesso digital reforçam a resiliência ciberfísica

Para implementar uma estrutura de segurança abrangente, as soluções digitais e em rede oferecem vantagens claras em relação aos sistemas mecânicos. Isto começa com a gestão simples de direitos e permissões de acesso para cada colaborador e estende-se à proteção contra furtos e até à segurança contra incêndios.

Especialmente na área da segurança física – protegendo colaboradores, ativos e dados analógicos e digitais contra ameaças externas e incidentes – **os sistemas de fecho digitais e as soluções eletrónicas de controlo de acessos (soluções de acesso digital)** oferecem maior conveniência e proteção reforçada.

As soluções de acesso digital podem contribuir de forma significativa para alcançar a conformidade com a Diretiva NIS2.

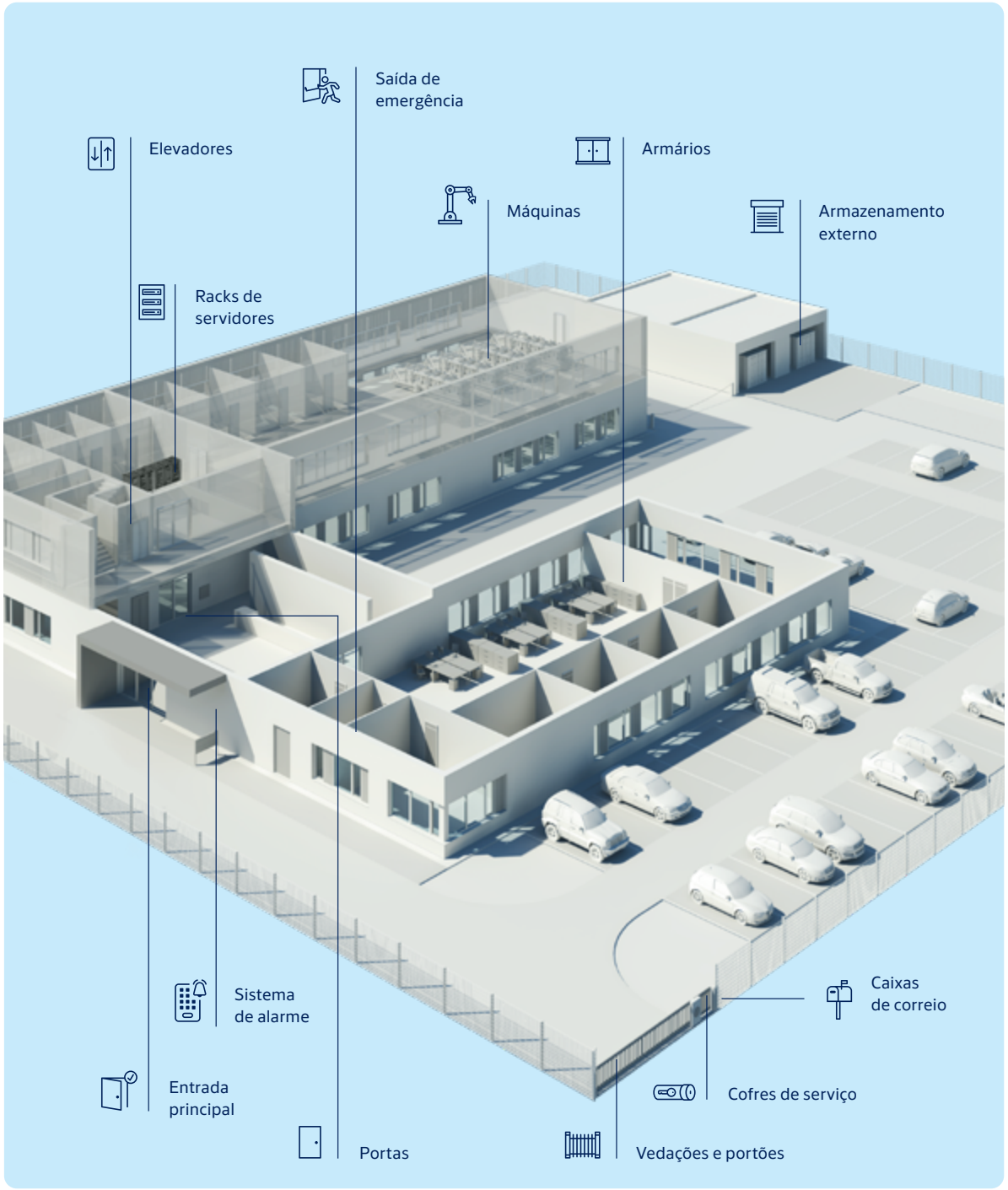
Reforçar a proteção desde o perímetro até ao núcleo

Segurança desde a primeira até à última linha de defesa – as soluções de acesso digital permitem proteger cada camada: tudo o que pode ser trancado deve estar protegido contra manipulação e ataques inteligentes.

Vantagens das Soluções de Acesso Digital da ASSA ABLOY – a proteger a sua organização e os seus dados:

- Controle quem vai aonde e quando, para cada utilizador, ou cancele credenciais perdidas com um clique
- Controlo de acessos online ou offline e melhoria de fluxos de trabalho através de uma gestão flexível, remotamente ou no local
- A oferta inclui sistemas de acesso digital ou hardware de acesso para atualizar um sistema existente
- Obtenha um controlo escalável sobre pontos de acesso que anteriormente eram inacessíveis
- A instalação simples de soluções sem fios não requer cablagem nem alterações estruturais
- Beneficie do nosso conhecimento aprofundado das normas regionais de portas e segurança
- A apoiá-lo na obtenção de conformidade com a NIS2
- Hardware de acesso para proteger as classes de proteção 1 a 4

Classe 1 Classe 2 Classe 3 Classe 4



Reforce o seu modelo de segurança com as soluções da ASSA ABLOY

A oferta de acesso digital da ASSA ABLOY inclui gestão de sistemas escalável, tipos de credenciais e hardware concebido para garantir a conformidade com a NIS2

Gestão do sistema disponível

As permissões de acesso podem ser definidas de forma flexível através da atribuição de direitos com sistemas de gestão intuitivos da ASSA ABLOY, que podem ser instalados localmente, na cloud ou em ambos. Se colaboradores ou um departamento inteiro se mudarem, não é necessário substituir as fechaduras. Credenciais perdidas deixam de representar um risco de segurança, pois podem simplesmente ser desativadas. Também são possíveis permissões de acesso baseadas no tempo e na localização — por exemplo, para conceder a técnicos uma autorização individual para uma tarefa específica. Em empresas de grande dimensão, pode ser útil emitir permissões de acesso com limite de tempo.

Tipos de credenciais disponíveis

Reforce a segurança ao escolher credenciais da ASSA ABLOY, como chaves inteligentes, cartões inteligentes, chaves móveis ou até biometria – e obtenha a flexibilidade de combinar múltiplas credenciais numa única solução de acesso.

Hardware de acesso disponível em vários formatos

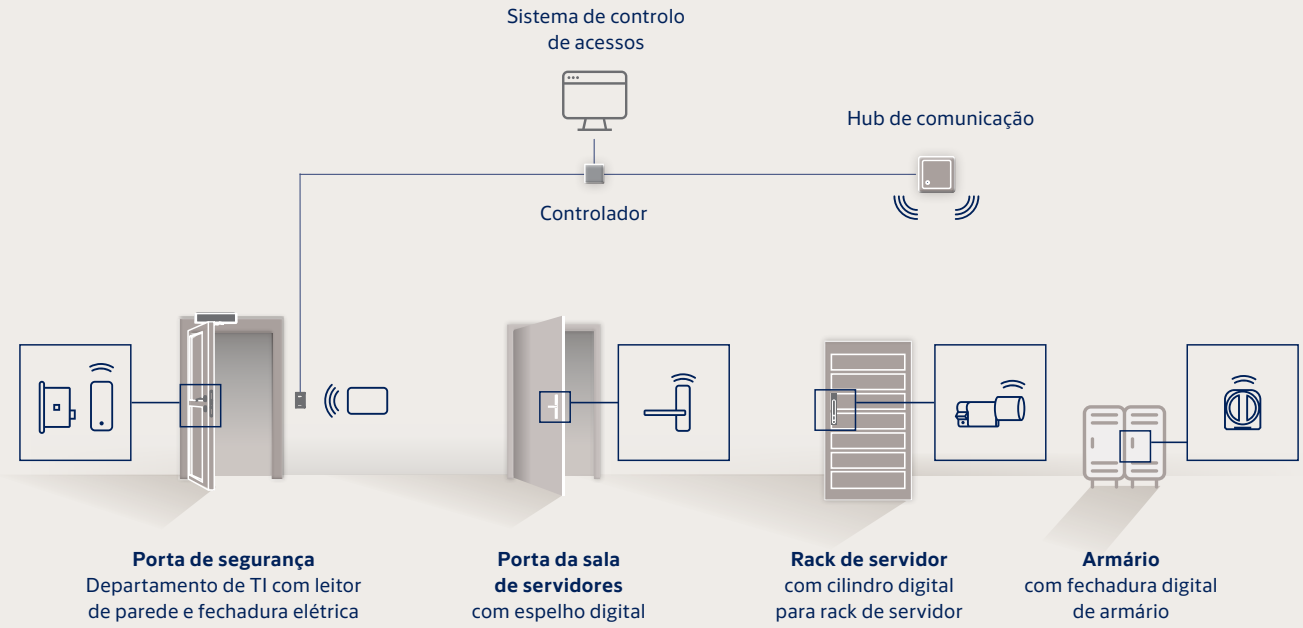
O hardware de acesso com fios e sem fios da ASSA ABLOY amplia o controlo flexível sobre mais pontos de entrada, dentro e fora do edifício, apoiando uma abordagem de segurança em camadas baseada no “princípio da casca de cebola”.

Caso de utilização: Proteger fisicamente uma área crítica com controlo de acessos digital

Departamento de TI e ativos

Classe de Proteção 4

Para proteger infraestruturas e ativos de TI sensíveis, a implementação de controlo de acessos digital garante que apenas pessoal autorizado consegue aceder fisicamente a áreas críticas. Esta abordagem reforça a segurança, apoia a conformidade e reduz o risco de violações de dados, ao integrar medidas de proteção física com políticas de TI.



Proteja ambientes de TI — incluindo racks de servidores — com proteção física robusta e controlo de acessos digital para salvaguardar dados sensíveis.

Uma visão geral das Soluções de Acesso Digital da ASSA ABLOY

Escolha o que melhor se adapta ao seu ambiente para reforçar a proteção do perímetro ao núcleo

Sistemas de gestão de acesso digital:

CLIQ®
Sistema simples baseado em chave que transforma um sistema mecânico numa gestão de acessos digital de alta segurança

SMARTair®
Solução moderna de acesso digital pronta a usar, que maximiza a flexibilidade e a facilidade de utilização

Hardware de acesso conectável para aumentar o controlo e a segurança:

Fechaduras Wireless Aperio®
A forma mais simples de expandir o alcance do seu sistema de controlo de acessos, sem necessidade de cabos ou obras

Escolha o que melhor funciona para si
Uma visão geral das funcionalidades e comparação

Ver página seguinte

Principais características do controlo de acesso físico ajudam a proteger colaboradores, ativos e dados, tanto analógicos como digitais, contra ameaças externas e incidentes	**Sistemas de gestão de acesso digital da ASSA ABLOY** **CLIQ®** Sistema simples baseado em chave que transforma um sistema mecânico numa gestão de acessos digital de alta segurança	**SMARTair®** Solução moderna de acesso digital pronta a usar, que maximiza a flexibilidade e a facilidade de utilização
Controlo de acessos e gestão de identidades garantem que apenas pessoas autorizadas podem aceder a sistemas, espaços ou dados específicos	✓	✓
Auditabilidade e rastreabilidade garantem que todas as ações críticas e acessos aos sistemas são registados e podem ser analisados – permitindo responsabilização, investigação de incidentes e verificação de conformidade	✓	✓
Credenciais digitais utilizadas para autenticar utilizadores, dispositivos ou sistemas e controlar o acesso a dados e serviços sensíveis	Chaves inteligentes, opcionais com RFID	Smart cards e fobs, chaves móveis, PIN, chaves inteligentes CLIQ
Revogação ou desativação de credenciais garante que os direitos de acesso são removidos rapidamente quando já não são necessários, protegendo os sistemas contra utilizações não autorizadas	✓	✓
Acesso remoto seguro garante que colaboradores e terceiros podem aceder remotamente a sistemas e dados críticos utilizando ligações encriptadas, autenticação forte e controlos de acesso rigorosos para evitar acessos não autorizados e fugas de dados	✓	✓
Comunicação segura / encriptação garante que os dados trocados entre dispositivos, credenciais e software estão protegidos por métodos criptográficos robustos, prevenindo acessos não autorizados, manipulação ou fugas de informação durante a transmissão	✓	✓
Hardware de acesso e classes de proteção protegem áreas com base num modelo de segurança em camadas	**Mais de 60 tipos de cilindros e cadeados** Alimentados por bateria na chave Classes de proteção: 1, 2, 3, 4	**Fechaduras, espelhos, cilindros, cadeados e leitores** Alimentados por bateria integrada no hardware de acesso Classes de proteção: 1, 2, 3, 4

Principais características do controlo de acesso físico ajudam a proteger colaboradores, ativos e dados, tanto analógicos como digitais, contra ameaças externas e incidentes	**Hardware de acesso conectável para aumentar o controlo e a segurança** **Aperio** A forma mais simples de expandir o alcance do seu sistema de controlo de acessos
Controlo de acessos e gestão de identidades garantem que apenas pessoas autorizadas podem aceder a sistemas, espaços ou dados específicos	✓
Auditabilidade e rastreabilidade garantem que todas as ações críticas e acessos aos sistemas são registados e podem ser analisados — permitindo responsabilização, investigação de incidentes e verificação de conformidade	✓
Credenciais digitais usadas para autenticar utilizadores, dispositivos ou sistemas e para controlar o acesso a dados e serviços sensíveis	Cartões inteligentes e fobs, chaves móveis, PIN
Revogação ou desativação de credenciais garante que os direitos de acesso são removidos rapidamente quando já não são necessários, protegendo os sistemas contra utilizações não autorizadas	✓
Acesso remoto seguro garante que colaboradores e terceiros podem aceder remotamente a sistemas e dados críticos, utilizando ligações encriptadas, autenticação forte e controlos de acesso rigorosos para evitar acessos não autorizados e fugas de informação	✓ Integrado em sistema de terceiros
Comunicação segura / encriptação garante que os dados trocados entre dispositivos, credenciais e software estão protegidos por métodos criptográficos robustos, prevenindo acessos não autorizados, manipulação ou fugas de informação durante a transmissão	✓
Hardware de acesso e classes de proteção protegem áreas com base num modelo de segurança em camadas	**Fechaduras, espelhos, cilindros, cadeados e leitores** Alimentados por bateria Classes de proteção: 1, 2, 3, 4

Hardware de acesso adicional e conectável para aumentar o controlo e a segurança

Ver página seguinte

Hardware de acesso adicional e conectável para aumentar o controlo e a segurança

Fechaduras Elétricas ABLOY®

Combinando robustez mecânica com controlo avançado, estas fechaduras elétricas são ideais para infraestruturas críticas e ambientes comerciais.

Reconhecidas mundialmente, integram-se com sistemas de acesso e alarme, consumindo energia apenas quando necessário para garantir uma proteção eficiente e certificada.

Fechaduras elétricas effeff

Projetadas para ambientes comerciais e de elevado fluxo de pessoas, as fechaduras elétricas effeff oferecem uma combinação fiável de robustez mecânica e inteligência digital.

Compactas, duráveis e digitalmente conectadas, integram-se com videoporteiros e sistemas de acesso para modernizar fechaduras mecânicas sem alterar a estrutura da porta.

Tecnologia eletrónica de vias de evacuação effeff

ePED® reúne segurança certificada com controlo inteligente e integrado — oferecendo soluções flexíveis para saídas de emergência modernas.

Design moderno, indicações visuais para utilização intuitiva e instalação simples combinam-se para modernizar a tecnologia de vias de evacuação em edifícios do século XXI. Desenvolvido para situações críticas, o ePED garante que as portas permanecem bloqueadas até autorização de abertura, orientando os utilizadores em segurança durante emergências.

Próximos passos: checklist de ações para conformidade com a NIS2

Fase	Item de ação	Detalhes / melhorias
Classificação e âmbito	Identificar se a sua organização é uma entidade “essencial” ou “importante”	Utilizar os códigos NACE e os limiares de dimensão; incluir subsidiárias e operações transfronteiriças
Governança e responsabilidade	Nomear uma pessoa ou equipa responsável pela conformidade com a NIS2	Definir funções para cibersegurança, segurança física e conformidade jurídica
Avaliação de risco	Realizar uma análise de risco ciberfísica abrangente	Incluir sistemas de TI, acesso físico, cadeia de abastecimento e dependências de terceiros
Estrutura de políticas	Desenvolver ou atualizar políticas e procedimentos de segurança	Incluir resposta a incidentes, continuidade do negócio, controlo de acessos e gestão de vulnerabilidades
Medidas técnicas e organizacionais	Implementar controlos adequados	Exemplos: MFA, encriptação, segmentação de rede, desenvolvimento seguro de software, controlo de acessos
Medidas de segurança física	Reforçar o controlo de acessos físicos e a segurança da infraestrutura Estruturar a segurança por camadas, com base no “princípio da casca de cebola”	Garantir segurança física através do controlo de acesso a áreas críticas, monitorização de atividade, proteção da infraestrutura e formação de equipas para manter a continuidade operacional e prevenir acessos não autorizados
Segurança da cadeia de abastecimento	Avaliar e proteger as relações com terceiros	Incluir cláusulas contratuais, auditorias e segmentação de fornecedores com base no risco
Resposta e comunicação de incidentes	Estabelecer procedimentos para deteção e comunicação de incidentes	Incidentes significativos devem ser comunicados ao CSIRT no prazo de 24 horas; manter registos e evidências
Continuidade do negócio e recuperação	Implementar planos de backup e recuperação após desastre	Testar regularmente; garantir resiliência contra ransomware e sabotagem física
Formação e sensibilização das equipas	Realizar formação regular em cibersegurança e segurança física	Incluir phishing
Monitorização da conformidade	Monitorizar continuamente o estado de conformidade com a NIS2 e corrigir rapidamente quaisquer situações de não conformidade	Avaliar e documentar regularmente as medidas de cibersegurança e segurança física, os riscos e as respostas a incidentes, para garantir que cumprem os requisitos da NIS2 e resistem a auditorias ou inspeções

Alcance a conformidade com a NIS2 com confiança. Os nossos especialistas estão aqui para ajudar

Convidamo-lo a contactar-nos para que possamos fornecer uma explicação detalhada sobre como as nossas soluções de acesso digital podem apoiar a conformidade com a Diretiva NIS2. Os nossos especialistas estão disponíveis para o orientar nas funcionalidades e benefícios que respondem aos requisitos da diretiva e reforçam o quadro de segurança ciberfísica da sua organização.

Independentemente de a sua empresa estar ou não abrangida pelos requisitos da Diretiva NIS2, investir numa solução moderna de acesso digital ajuda a reforçar a proteção de informação e ativos próprios, bem como de dados específicos de clientes.

As suas questões são importantes — fale connosco

Prepare os seus acessos para o futuro

Digital with confidence

Versão: AA_DAS_NIS2_Whitepaper_2026-03_PT

A ASSA ABLOY está empenhada em cumprir a Diretiva NIS2 da União Europeia. Implementámos medidas robustas de cibersegurança para proteger os nossos sistemas e dados. A nossa abordagem inclui gestão de riscos, resposta a incidentes e controlo de acessos. O nosso alinhamento com a ISO/IEC 27001 e outras normas relevantes reforça o nosso compromisso com a resiliência, a confiança e a conformidade regulamentar.

ASSA ABLOY Opening Solutions

Lisboa
Rua Cidade de Córdova, 3ª Zona
Industrial de Alfragide Sul
2610-038 Alfragide
Tel: +351 215 966 888

Porto
Rua Hintze Ribeiro, 585
Sala 305
4450-692 Leça da Palmeira
Tel.: +351 229 998 980

Águeda
Zona industrial de Alagoa
Apartado 3134
3754-901 Águeda

geral.portugal@assaabloy.com
www.assaabloy.com

Experience a safer
and more open world

ASSA ABLOY