Roadmap para a conformidade NIS2 / SRI2

O caminho para a conformidade com a Diretiva NIS2 / SRI2 a percorrer pelas organizações

devoteam
Cyber Trust

A Diretiva NIS2 / SRI2 estabelece a base de referência para as medidas de gestão dos riscos de cibersegurança e as obrigações de notificação nos setores abrangidos pelo respetivo âmbito de aplicação.

As medidas de gestão dos riscos de cibersegurança deverão ter em consideração o grau de dependência da entidade essencial ou importante em relação aos sistemas de rede e informação e incluir medidas para identificar os riscos de incidentes, para evitar e detetar os incidentes, bem como para lhes dar resposta, permitir a recuperação após estes incidentes e atenuar o seu impacto. A segurança dos sistemas de rede e informação deverá abranger a segurança dos dados armazenados, transmitidos e tratados.

Os principais requisitos e obrigações para as organizações são:

- Processo de gestão dos riscos de segurança da informação e cibersegurança;
- Avaliação da eficácia das medidas de mitigação dos riscos de segurança da informação e cibersegurança;
- Gestão de incidentes de segurança da informação e cibersegurança;
- Gestão da continuidade de negócio;
- Segurança da cadeia de abastecimento;
- Segurança na aquisição, desenvolvimento e manutenção;
- Práticas básicas de ciber-higiene e formação em cibersegurança;
- Gestão de acessos e utilização de soluções de autenticação multifatores ou de autenticação contínua;
- Criptografia e, se for caso disso, decifragem;
- Segurança dos recursos humanos.

Roadmap para a conformidade NIS2 / SRI2 é um serviço especializado que tem como objetivo suportar as organizações em todas as atividades que devem desenvolver tendo como objetivo cumprir os requisitos e obrigações impostos pela Diretiva NIS2 / SRI2.

Ao longo de um período de tempo, a determinar em função do contexto e âmbito de aplicação em cada organização, serão executadas atividades de avaliação do estágio de conformidade/maturidade, elaboração de informação documentada obrigatória, estabelecimento/consolidação de um processo de Gestão de Risco, estabelecimento/consolidação de um processo de Gestão de Incidentes e de operacionalização de todos os processos de operação e gestão continuados preconizados pela Diretiva NIS2 / SRI2.

O nosso enfoque é proporcionar uma ajuda especializada e experiente face às necessidades específicas de cada organização tendo como objetivo final a conformidade com a Diretiva NIS2 / SRI2.

Roadmap para a conformidade NIS2 / SRI2

01
Definir o âmbito de aplicação da NIS2 / SRI2

02
Realizar uma avaliação da conformidade / maturidade da NIS2 / SRI2

03
Definir e operacionalizar políticas e procedimentos

04
Estabelecer / consolidar um processo de Gestão de Risco

05
Estabelecer / consolidar um processo de Gestão de Incidentes

06
Gerir a conformidade com a NIS2 / SRI2

Requisitos

Duração Estimada

Depende do contexto e do âmbito de cada organização.

"Ponto de Contacto Designado": As entidades devem designar um ponto de contacto que será responsável por coordenar a interação entre a nossa equipa de consultores e todas as unidades de negócio da organização envolvidas na prestação de serviços pelos quais são consideradas entidades essenciais ou importantes pela Diretiva NIS2 / SRI2.

"Acesso a Documentação": Os nossos consultores precisam de ter acesso à documentação relevante, incluindo políticas de segurança, procedimentos de gestão de riscos, e configurações de sistemas e redes, conforme necessário.

"Disponibilidade de Equipas": É necessário que os membros de todas as unidades de negócio da organização envolvidas na prestação de serviços estejam disponíveis para sessões de trabalho periódicas, consultas e esclarecimentos sobre os serviços e infraestrutura de TIC de suporte aos mesmos.

"Compromisso com a Segurança": É importante que a organização demonstre compromisso com a melhoria da cibersegurança, estando aberta a receber feedback e disposta a considerar as recomendações fornecidas.

Entregáveis

01

Definir o âmbito de aplicação da NIS2 / SRI2

- Identificar serviços essenciais / importantes / atividades críticas
- Identificar os ativos de informação relacionados

02

Realizar uma avaliação da conformidade / maturidade da NIS2 / SRI2

- Identificar os GAPs que a organização pode ter em relação aos requisitos e obrigações da NIS2 / SRI2
- Identificar as mesmas lacunas no que respeita à cadeia de fornecimento

03

Definir e operacionalizar políticas e procedimentos

- Políticas em matéria de análise de riscos e segurança dos sistemas de informação
- Procedimentos de gestão de incidentes
- Políticas e procedimentos de continuidade do negócio, tais como gestão de cópias de segurança, disaster recovery, e gestão de crises
- Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança
- Políticas e procedimentos relativos à utilização da criptografia
- Segurança dos recursos humanos, políticas de controlo de acesso e gestão de ativos

04

Estabelecer / consolidar um processo de Gestão de Risco

- Operacionalizar a metodologia de Gestão de Risco
- Realizar uma iteração de gestão de riscos
- Estabelecer um plano de tratamento dos riscos

05

Estabelecer / consolidar um processo de Gestão de Incidentes

- Operacionalizar os procedimentos de gestão de incidentes
- Estabelecer os mecanismos internos e externos de notificação de incidentes

06

Gerir a conformidade com a NIS2 / SRI2

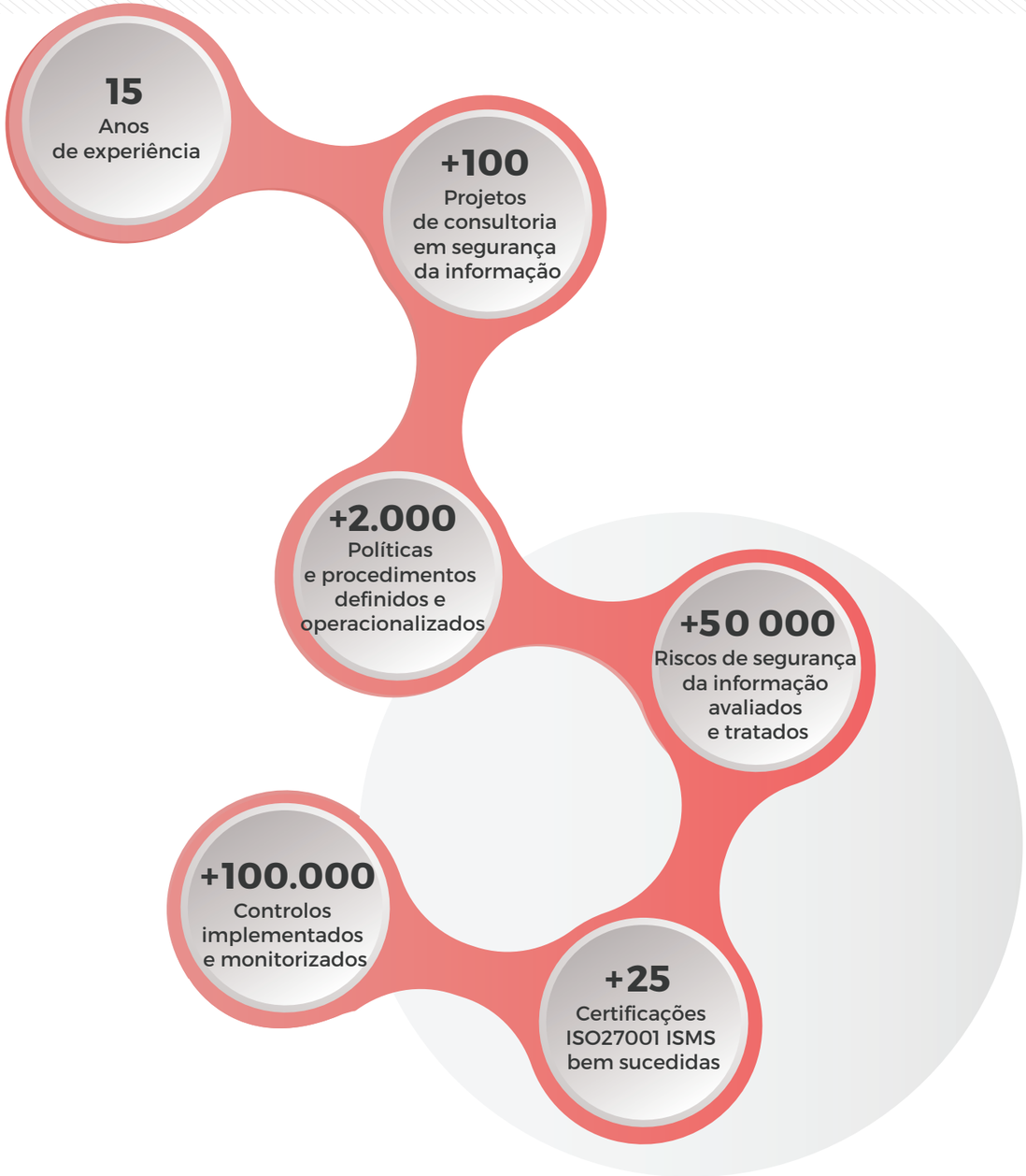
- Caracterizar o(s) conjunto(s) de requisitos de conformidade aplicáveis da NIS2 / SRI2 (compliance trees)
- Mapear o(s) conjunto(s) de requisitos de conformidade (compliance trees) com os recursos, atividades e evidências relacionados.
- Mapear o(s) conjunto(s) de requisitos de conformidade (compliance trees) com outras normas, tais como. ISO27K, NIST CSF, ISA/IEC 62443, etc.

A nossa experiência

Durante mais de 15 anos, a nossa prática de consultoria em cibersegurança tem ajudado empresas de uma vasta gama de setores a gerir proativamente os seus riscos de cibersegurança. Ajudámos dezenas de empresas a avaliar e a mitigar milhares de riscos e elaborámos centenas de políticas e procedimentos para garantir a conformidade com os regulamentos e normas de cibersegurança.

A nossa equipa de especialistas em cibersegurança tem uma vasta experiência de trabalho com clientes B2B de grande e média dimensão, e possuímos certificações relevantes, tais como ISO 27001 LA/LI, CISA, CISM, CRISC, CDPSE e outras. Temos um entendimento profundo do panorama da cibersegurança em evolução e mantemo-nos atualizados com as últimas ameaças, tendências e regulamentos.

Adotamos uma abordagem personalizada à consultoria de cibersegurança, trabalhando em estreita colaboração com os nossos clientes para compreender as suas necessidades únicas e desenvolver soluções personalizadas que atenuem os riscos e melhorem a sua postura de cibersegurança. O nosso historial de sucesso comprovado fala por si e estamos empenhados em fornecer serviços de consultoria de cibersegurança da mais elevada qualidade aos nossos clientes.



Certificações
& Clientes

Apoiada numa carteira diversificada de clientes globais e numa ampla gama de certificações, incluindo CREST, ISO 27001, ISO 27701, ISO 9001 e PCI QSA, a Devoteam Cyber Trust é a principal opção para organizações que procuram o mais alto nível de especialização em serviços segurança ofensiva.

ISO 27001 (2012)

CREST (2014)

ISO 9001 (2014)

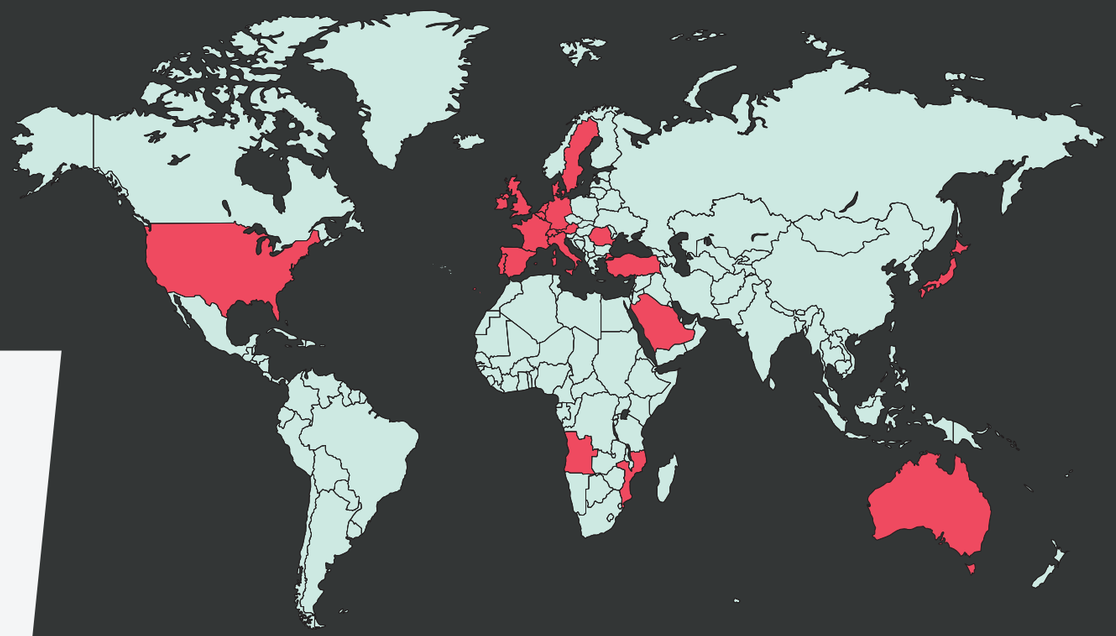
PNSC (2017)

PCI (2020)

Bancontact (2021)

ISO 27701 (2023)

EPI (2024)



Mais de 20 países em todo o mundo

Com sede em Lisboa, prestamos serviços a um **grande número de empresas de grande e média dimensão**, tanto a nível nacional como internacional.

Porquê colaborar com a Devoteam Cyber Trust

- Profundos conhecimentos e experiência em consultoria de cibersegurança, com mais de 15 anos de experiência líder no setor.
- Uma equipa de profissionais de segurança altamente certificados e experientes, incluindo especialistas em ISO 27001, NIS2 e RGPD, que fornecem soluções personalizadas para satisfazer as necessidades e objetivos únicos de cada organização.
- Cobertura abrangente e flexibilidade, com uma vasta gama de serviços de consultoria e metodologías adaptadas aos riscos e desafios específicos de cibersegurança que a sua organização enfrenta.
- Um compromisso com a qualidade e a excelência, com foco no fornecimento dos mais altos níveis de serviço e satisfação do cliente.
- Acesso a tecnologia e ferramentas avançadas, incluindo a nossa ferramenta proprietária IntegrityGRC, para ajudar os clientes a gerir os seus requisitos de governação, risco e conformidade.
- Conformidade com as normas e regulamentos do setor, incluindo ISO27001, NIS2, RGPD e outras diretrizes e estruturas relevantes, para ajudar os clientes a reduzir os riscos de cibersegurança e evitar penalizações e responsabilidades legais.
- Um enfoque em parcerias de longo prazo e apoio contínuo, com monitorização e relatórios continuados que fornecem feedback contínuo e capacidades de gestão de riscos.
- Uma presença e reputação globais, com clientes em mais de 20 países e um historial comprovado de prestação de serviços de consultoria de cibersegurança eficazes e de elevada qualidade.

Devoteam Cyber Trust é o parceiro certo para apoiar a sua organização neste cenário de ameaças intenso e em constante evolução, com Serviços de Segurança Ofensiva de classe mundial.

É por isso que dezenas de clientes de média e grande dimensão em mais de 20 países em todo o mundo confiam nos nossos serviços.

Estamos disponíveis para partilhar a nossa **experiência** e ajudá-lo a melhorar as suas práticas de **cibersegurança.**

A gestão equilibrada dos riscos requer uma estratégia sólida.

Fale connosco.

Contacte-nos

info@integrity.pt

Presentes em mais de 12 países da EMEA

www.integrity.pt

devoteam Cyber Trust

About devoteam Cyber Trust

www.integrity.pt

www.devoteam.com/expertise/cyber-trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e CIS - Centro de Segurança na Internet, prestamos serviços a um número considerável de clientes, operando em mais de 20 países.

Sobre devoteam

www.devoteam.com

A Devoteam é uma empresa líder em consultoria focada em estratégia digital, plataformas tecnológicas e cibersegurança.

Ao combinar criatividade, tecnologia e insights de dados, capacitamos nossos clientes a transformar os seus negócios e desbloquear o futuro.

Com 25 anos de experiência e 10.000 funcionários em toda a Europa, Oriente Médio e África, a Devoteam promove tecnologia responsável para as pessoas e trabalha para criar mudanças positivas.

Creative tech for Better Change.