MANUAL DO ALUNO

Cybersecurity de Ponta a Ponta

Guia completo da sua jornada de aprendizado

11	58h	3	14
Módulos	de Conteúdo	Certificações	Conquistas

W2CONN Consultoria em Tecnologia e Cibersegurança — 2026

Sumário

Navegue pelo manual e descubra tudo sobre sua jornada.

01 **Bem-vindo à W2CONN**

02 **Primeiros Passos na Plataforma**

03 **Estrutura do Curso e Módulos**

04 **Recursos de Aprendizado**

05 **Biblioteca Virtual**

06 **Estudo de Caso: Cacau Choc**

07 **Tutor IA — Seu Assistente Pessoal**

08 **Sistema de Conquistas e Badges**

09 **Certificações Profissionais**

10 **Carga Horária e Planejamento de Estudo**

11 **Dashboard e Acompanhamento de Progresso**

Introdução | Fundamentos | Prático | Governança

> 💡 **Dica:** Este manual foi pensado para acompanhar você do primeiro ao último dia de curso. Consulte-o sempre que precisar!

01 — Bem-vindo à W2CONN

Sua jornada em cibersegurança começa agora.

A **W2CONN Consultoria em Tecnologia e Cibersegurança** é referência em formação profissional na área de segurança da informação. Nosso curso **"Cybersecurity de Ponta a Ponta"** foi desenvolvido para capacitar profissionais com conhecimentos que vão desde os fundamentos da segurança digital até a governança estratégica corporativa.

O que você vai aprender?

- ✓ Fundamentos de Segurança da Informação (Tríade CID, ISO 27001)
- ✓ Engenharia Social e proteção do fator humano
- ✓ Frameworks modernos: NIST CSF 2.0, OWASP Top 10, CIS Benchmarks
- ✓ Hardening de sistemas e resposta a incidentes (ISO 27035)
- ✓ Compliance e LGPD na prática
- ✓ Governança de SI e Gestão de Riscos (COBIT 2019, FAIR)

Para quem é este curso?

Profissionais de TI, gestores, analistas de segurança, consultores e qualquer pessoa que deseja construir uma carreira sólida em cibersegurança. Não é necessário conhecimento prévio — o curso parte do básico ao avançado.

Metodologia

Nosso método combina **teoria contextualizada** com um **estudo de caso real (Cacau Choc)** que permeia todos os módulos. Você aprende aplicando conceitos em cenários reais, com quizzes, flashcards, atividades práticas e o suporte de um tutor IA especializado.

> 💡 **Diferencial:** O curso é baseado no caso real de uma empresa em preparação para um IPO de R$ 1,2 bilhão — você vivencia desafios reais de cibersegurança corporativa.

02 — Primeiros Passos

Como se cadastrar, acessar e navegar na plataforma.

Cadastro e Acesso

1. **Acesse a plataforma** em **cyber.w2conn.com.br**
2. **Clique em "Começar Agora"** na página inicial para criar sua conta.
3. **Preencha seus dados:** nome completo, e-mail corporativo e uma senha forte (mínimo 8 caracteres, com maiúsculas, minúsculas e números).
4. **Aceite os termos LGPD** — você será direcionado à tela de consentimento de dados na primeira vez.
5. **Pronto!** Você será redirecionado ao seu Dashboard pessoal.

> 💡 **Alternativa:** Você também pode cadastrar-se usando sua conta Google, clicando em "Cadastrar com Google".

Navegação Principal

Após o login, o menu principal dá acesso a todas as áreas:

📊 Dashboard

Visão geral do seu progresso, módulos em andamento e próximos passos.

📚 Módulos

Acesso à lista completa dos 11 módulos do curso.

📖 Biblioteca

Materiais de apoio: PDFs, infográficos e links de referência.

🏢 Estudo de Caso

O caso completo da Cacau Choc para estudo contextualizado.

🏆 Conquistas

Seus badges e certificados obtidos ao longo do curso.

👤 Perfil

Suas informações pessoais, estatísticas e configurações de segurança.

03 — Estrutura do Curso

11 módulos organizados em 4 níveis progressivos.

🟢 Nível: Introdução

0 **Cybersecurity de Ponta a Ponta na Cacau Choc**

Conheça o estudo de caso que guiará todo o curso: a empresa Cacau Choc, seus desafios e a preparação para o IPO.

⏱ 3 horas

🔵 Nível: Fundamentos (Módulos 1-3)

1 **O Admirável Mundo Digital e Suas Sombras**

Fundamentos da segurança da informação, Tríade CID e a importância da ISO 27001.

⏱ 4 horas

2 **O Fator Humano e a Engenharia Social**

Vulnerabilidades humanas e técnicas de engenharia social: phishing, vishing, smishing.

⏱ 4 horas

3 **Anatomia da Proteção (ISO 27001 Fundamentals)**

SGSI, ciclo PDCA e os 93 controles do Anexo A da ISO 27001.

⏱ 5 horas

🟣 Nível: Prático (Módulos 4-8)

4 **Defesa Profunda com NIST CSF 2.0 e IA**

As 5 funções do NIST CSF e defesa em camadas para proteção organizacional.

⏱ 6 horas

5 **Segurança em Aplicações (OWASP)**

As 10 vulnerabilidades mais críticas de aplicações web segundo o OWASP.

⏱ 8 horas

6 **Hardening e Configuração Segura**

CIS Benchmarks, PAM e DLP para configuração segura de sistemas.

⏱ 6 horas

7 **Resposta a Incidentes de Segurança**

ISO 27035 e metodologia PICERL para processos de resposta a incidentes.

⏱ 6 horas

8 **Auditoria e Compliance (LGPD)**

Conformidade com a LGPD e preparação para auditorias.

⏱ 5 horas

🟡 Nível: Governança (Módulos 9-10)

9 **Governança de Segurança da Informação**

Alinhe segurança com objetivos de negócio usando frameworks de governança.

⏱ 5 horas

10 **Gestão de Riscos de Segurança da Informação**

Metodologia FAIR, cálculo de ROI de segurança e gestão de riscos.

⏱ 6 horas

04 — Recursos de Aprendizado

Ferramentas interativas para maximizar seu aprendizado.

Cada módulo oferece uma variedade de recursos para reforçar o conteúdo. Aqui está o que você encontrará:

📝 Quizzes Avaliativos

Cada módulo possui um quiz com questões de múltipla escolha, pesos diferenciados e correção automática. Você precisa atingir **nota ≥ 7,0** para receber o badge de "Conquistador" do módulo. Pode refazer quantas vezes desejar — sua melhor nota é salva.

🃏 Flashcards

Cada módulo conta com aproximadamente **15 flashcards** com conceitos-chave para revisão rápida. Clique no card para revelar a resposta e reforce sua memorização com a técnica de repetição espaçada.

🎯 Atividades Práticas

Exercícios aplicados ao contexto da Cacau Choc. Você avalia cenários, propõe soluções e recebe feedback. As atividades são salvas automaticamente no seu progresso.

🎧 Áudios

Alguns módulos contam com conteúdo em áudio, ideal para estudar em trânsito. Acesse pelo ícone de fone de ouvido no cabeçalho de cada módulo.

📌 Notas Pessoais

Crie anotações vinculadas a cada módulo. Na aba **"Notas"** dentro de cada módulo, você pode criar, editar e excluir anotações para registrar insights e pontos importantes.

🔖 Favoritos (Bookmarks)

Marque módulos como favoritos clicando no ícone de marcador no cabeçalho. Isso facilita encontrar rapidamente os módulos que você mais acessa ou deseja revisar.

💡 **Estratégia recomendada:** Estude o conteúdo → Revise com flashcards → Faça a atividade prática → Realize o quiz. Essa sequência maximiza a retenção do conhecimento.

05 — Biblioteca Virtual

Materiais complementares para aprofundar seu conhecimento.

A Biblioteca Virtual reúne todos os materiais de apoio do curso, organizados por categoria. Acesse pelo menu principal.

📄 Apresentações em PDF

Apresentações detalhadas de cada módulo, disponíveis para visualização no navegador e download. Inclui slides com resumos, diagramas e frameworks completos.

🔗 Links de Referência

Curadoria de referências externas essenciais para o profissional de cibersegurança:

- ✓ **OWASP Top 10** — As vulnerabilidades mais críticas em aplicações web
- ✓ **NIST Cybersecurity Framework** — Framework de cibersegurança do governo americano
- ✓ **LGPD (Lei nº 13.709/2018)** — Legislação brasileira de proteção de dados
- ✓ **CIS Benchmarks** — Guias de configuração segura para sistemas
- ✓ **ISO/IEC 27001** — Padrão internacional de gestão de segurança da informação

📊 Infográficos

Resumos visuais dos principais conceitos, ideais para revisão rápida e consulta durante atividades práticas.

> 💡 **Dica:** Utilize os PDFs da biblioteca como material de consulta durante os quizzes — o objetivo é aprender, não decorar!

06 — Estudo de Caso: Cacau Choc

Aprenda com um cenário corporativo real.

O coração do curso é o estudo de caso da **Cacau Choc**, uma fabricante de chocolates premium em preparação para um **IPO de R$ 1,2 bilhão**. A empresa enfrenta desafios críticos de cibersegurança que colocam em risco não apenas seus dados, mas toda a operação de abertura de capital.

Seções do Estudo de Caso

🏭 Histórico da Empresa

Da fundação familiar à multinacional com faturamento bilionário.

⚡ Situação Atual

Os desafios de segurança que surgiram com o crescimento acelerado.

👥 Personagens

Mais de 10 stakeholders envolvidos: do CEO ao estagiário de TI.

🔓 Incidentes de Segurança

Casos reais de violações que a empresa precisou enfrentar.

📈 Preparação para o IPO

Como a cibersegurança se tornou fator decisivo para os investidores.

Como Utilizar o Estudo de Caso

O caso está integrado a todos os módulos. Cada tema estudado será aplicado ao contexto da Cacau Choc por meio de atividades práticas. Você pode acessar o caso completo pelo menu **"Estudo de Caso"** a qualquer momento para consultar detalhes durante as atividades.

> 💡 **Imersão:** Imagine-se como consultor(a) contratado(a) pela Cacau Choc. Cada módulo apresenta um novo desafio — e você deve propor a solução.

07 — Tutor IA

Seu assistente pessoal de cibersegurança.

Cada módulo conta com um **Tutor IA especializado**, disponível na aba de chat dentro de cada módulo. Ele foi treinado com o conteúdo do curso e pode ajudá-lo de diversas formas.

O que o Tutor IA pode fazer?

- ✓ Explicar conceitos do módulo de forma simples e com exemplos
- ✓ Tirar dúvidas sobre frameworks (ISO 27001, NIST CSF, OWASP)
- ✓ Ajudar a interpretar cenários do estudo de caso
- ✓ Dar dicas sobre como abordar atividades práticas
- ✓ Fornecer contexto adicional sobre termos técnicos
- ✓ Sugerir estratégias de estudo personalizadas

Como acessar

1. Entre em qualquer módulo pelo menu "Módulos".
2. Clique na aba **"Chat IA"** na área de conteúdo.
3. Digite sua pergunta e envie — o tutor responde em segundos.

> 💡 **Aproveite:** Use o tutor antes dos quizzes para revisar conceitos ou após um resultado baixo para entender onde errou. O tutor é contextualizado ao módulo que você está estudando.

08 — Sistema de Conquistas

14 badges para reconhecer seu progresso.

A plataforma premia seu avanço com badges (emblemas) que reconhecem cada etapa conquistada.

Badge Inicial

🎖️ **Empreendedor**

Concedido automaticamente ao se cadastrar no curso.

Badges de Módulo (10 badges)

Um badge **"Conquistador"** para cada módulo (1 a 10), obtido ao completar o quiz com **nota ≥ 7,0**.

Badges Especiais

🏅 Fundamentos Completos

Completar os módulos 1, 2 e 3.

🛡️ Prático em Segurança

Completar os módulos 4 a 8.

🏆 Expert em Cybersecurity

Completar todos os módulos (1-10) com média ≥ 7,5.

> 💡 **Acompanhe:** Veja todos os seus badges na página **"Conquistas"** do menu. Badges não conquistados aparecem como bloqueados com os requisitos visíveis.

09 — Certificações Profissionais

3 certificados reconhecidos para validar sua expertise.

Ao completar grupos de módulos, você pode solicitar certificados oficiais da W2CONN. Cada certificado possui um **código de validação único** que pode ser verificado publicamente.

NÍVEL 1
Fundamentos
ISO 27000
Módulos 0-3

NÍVEL 2
Avançado
OWASP, NIST CSF & ISO
Módulos 4-8

NÍVEL 3
Governança
COBIT 2019
Módulos 9-10

Como obter seu certificado

1. **Complete todos os módulos** do nível desejado com aprovação nos quizzes.
2. **Acesse seu Perfil** e vá até a seção de Certificados.
3. **Solicite a emissão** do certificado — ele passará por aprovação.
4. **Após aprovação**, faça o download do certificado em PDF com design profissional.

Validação Pública

Cada certificado possui um número único (ex: `W2C-FUND-2024-00001`) que pode ser verificado por terceiros na página de validação pública da plataforma. Compartilhe em seu LinkedIn ou currículo com confiança.

> 💡 **Estratégia:** Comece pelo Certificado de Fundamentos — ele valida conhecimentos essenciais e já é um diferencial no mercado.

10 — Carga Horária e Planejamento

58 horas de conteúdo no seu ritmo.

Distribuição de Horas

Nível	Módulos	Horas
🟢 Introdução	Módulo 0	**3h**
🔵 Fundamentos	Módulos 1-3	**13h**
🟣 Prático	Módulos 4-8	**31h**
🟡 Governança	Módulos 9-10	**11h**
Total		**58h**

Sugestões de Ritmo de Estudo

⚡ Ritmo Intensivo (4 semanas)

~2 horas por dia, 7 dias por semana. Ideal para quem tem urgência ou disponibilidade integral.

📅 Ritmo Regular (8 semanas)

~1 hora por dia, 7 dias por semana. Bom equilíbrio entre estudo e rotina profissional.

🐢 Ritmo Flexível (12 semanas)

~45 min por dia, 5 dias por semana. Para quem precisa conciliar com outras atividades.

> 💡 **Recomendação:** Estude pelo menos 1 módulo completo antes de passar ao próximo. A sequência foi planejada para construir conhecimento progressivo.

11 — Dashboard e Progresso

Acompanhe cada passo da sua evolução.

O Dashboard é a sua central de controle. Ao fazer login, você verá imediatamente:

Informações Exibidas

- ✓ **Progresso Geral** — percentual de conclusão de todo o curso
- ✓ **Módulos Concluídos** — quantos módulos já completou
- ✓ **Pontuação Total** — soma das suas notas nos quizzes
- ✓ **Badges Conquistados** — total de emblemas obtidos
- ✓ **Próximo Módulo** — sugestão automática de onde continuar
- ✓ **Lista de Módulos** — status individual de cada módulo (não iniciado, em andamento, concluído)

Status dos Módulos

Cada módulo pode ter um dos seguintes status:

⬜ **Não Iniciado**
Módulo disponível, ainda sem acesso.

🔵 **Em Andamento**
Você já acessou e está estudando.

🟢 **Concluído**
Quiz aprovado com nota ≥ 7,0.

🟡 **Em Breve**
Módulo ainda não disponível.

Perfil e Estatísticas

Na página de **Perfil**, você encontra estatísticas detalhadas, histórico de quizzes realizados e pode gerenciar suas configurações de segurança (alterar senha, vincular conta Google).

Pronto para começar?

Acesse **cyber.w2conn.com.br** e inicie sua jornada em cibersegurança.

W2CONN Consultoria em Tecnologia e Cibersegurança — Todos os direitos reservados.