



CIBERSEGURANÇA E CULTURA ORGANIZACIONAL

**20 A 24 ABRIL
LISBOA**

PROGRAMA DE CURSO

Objetivos Gerais

Capacitar funcionários administrativos e gestores para identificarem, prevenirem e reagirem a ameaças digitais, transformando a segurança da informação numa vantagem estratégica e parte integrante da cultura organizacional, minimizando o risco de perdas financeiras e danos reputacionais.

Objetivos Específicos

No final da formação, os participantes deverão ser capazes de:

1. Consciencialização e Mentalidade (Cultura)
2. Prevenção de Ataques (Técnico-Comportamental)
 - Identificar tentativas de Engenharia Social
 - Gerir Identidades Digitais
 - Garantir a Higiene Digital
3. Gestão e Conformidade (Para Gestores)
 - Avaliar o Risco de Negócio
 - Aplicar o RGPD no Quotidiano
 - Gerir Shadow IT
4. Resposta e Continuidade
 - Executar o Protocolo de Incidente
 - Contribuir para a Continuidade.

O Capital Humano como Primeira Linha de Defesa

Este curso foi desenhado para todos os elementos da organização, independentemente da sua função, departamento ou nível de responsabilidade. Num era em que a transformação digital é transversal a todas as áreas, a cibersegurança deixou de ser uma tarefa exclusiva do departamento de IT para se tornar uma competência fundamental de cada colaborador.

Este programa é dirigido a:

- **Colaboradores de todas as áreas:** Que pretendem navegar no mundo digital com maior confiança, protegendo tanto a informação da empresa como os seus próprios dados pessoais.
- **Gestores e Líderes de Equipa:** Que têm a missão de fomentar uma cultura de vigilância e garantir que as boas práticas fazem parte da rotina operacional das suas equipas.
- **Direção e Tomadores de Decisão:** Que encaram a cibersegurança como um pilar estratégico para a resiliência do negócio, a reputação da marca e o cumprimento rigoroso do RGPD.
- **Novos Talentos:** Que, ao integrarem a organização, devem alinhar-se de imediato com os padrões de segurança e a ética digital que definem a nossa cultura organizacional.

Nota: Não são necessários conhecimentos técnicos avançados. O curso foca-se em comportamentos, atitudes e na compreensão dos riscos reais do quotidiano corporativo em Portugal e no mundo.

PROGRAMA

O percurso de aprendizagem está organizado em sete módulos complementares, que garantem uma visão 360° da organização:

Dia 1: **O Fator Humano e o Cenário de Ameaças**

- Contextualização: Por que as empresas são atacadas? (Motivações financeiras vs. espionagem).
- A "Firewall Humana": O papel crucial do administrativo na defesa da empresa.
- Engenharia Social: Anatomia de um ataque de Phishing, Smishing e Vishing.
- Atividade Prática: Análise real de e-mails suspeitos e identificação de sinais de alerta.

Dia 2: **Gestão de Identidade e Higiene Digital**

- Password Management: O fim da era da password simples; uso de gestores de passwords.
- MFA (Autenticação Multi-fator): Por que é a ferramenta de defesa mais importante hoje.
- Segurança no Posto de Trabalho: Bloqueio de ecrã, perigos de pens USB desconhecidas e Wi-Fi público.
- Atividade Prática: Configuração assistida de segurança em contas de teste.

Dia 3: **Proteção de Dados e Privacidade** (RGPD na Prática)

- Classificação de Informação: O que é público, interno, confidencial ou sensível.
- Fugas de Dados: Como ocorrem (ex: erro no CC do e-mail) e como evitar.
- Shadow IT: Os perigos de usar ferramentas não autorizadas (WhatsApp, Dropbox pessoal) para dados da empresa.
- Workshop: Simulação de manuseamento de dados sensíveis de clientes.

PROGRAMA

Dia 4: **Prevenção de Fraude Financeira e de Processos**

- CEO Fraud & BEC (Business Email Compromise): Como os atacantes se fazem passar por diretores para desviar pagamentos.
- Fraude de Faturas: Verificação de IBANs e processos de dupla autorização.
- Trabalho Remoto Seguro: Boas práticas em ambiente doméstico e em viagem.
- Estudo de Caso: Análise de uma fraude financeira real e onde falhou o processo humano.

Dia 5: **Resposta a Incidentes e Cultura de Reporte**

- Cultura do “No Blame”: Incentivar o reporte rápido em vez do medo da punição.
- Plano de Resposta: Identifiquei algo estranho, e agora? Quem contactar?
- Simulação Final (Tabletop): Exercício de grupo onde os gestores e administrativos têm de decidir o que fazer perante um ataque de Ransomware em curso.
- Encerramento: Entrega de “Checklists de Bolso” da Insignis West.

- Almoço Executivo, com entrega de Diplomas de Curso

INSCRIÇÃO

Informações de Inscrição

Disponibilizamos todos os dados essenciais para o processo de inscrição nas nossas ofertas formativas. Neste contexto, apresentamos as condições gerais:

Investimento e Condições de Pagamento

- Valor da Inscrição: Para obter informações detalhadas sobre valores e campanhas em vigor, solicitamos que consulte a nossa área de Formação Certificada através dos e-mails: formacao@insigniswest.com ou luanda.office@insigniswest.com.
- Modalidade de Pagamento: O pagamento deverá ser efetuado exclusivamente por transferência bancária.

O que está incluído?

Ao inscrever-se nesta formação, terá acesso a:

- Sessões de formação especializadas;
- Documentação de apoio em formato digital;
- Certificado/**Diploma Oficial** de conclusão de **Curso de Cibersegurança e Cultura Organizacional**.

Certificação

A Insignis West afirma-se como uma entidade devidamente **Acreditada e Certificada**, o que assegura os mais elevados padrões de qualidade em todos os seus processos formativos. Nesse sentido, importa destacar que o nosso corpo docente é composto exclusivamente por **formadores certificados**, que aliam uma vasta experiência profissional à excelência científica e pedagógica nas suas respetivas áreas de especialidade.

Desta forma, garantimos que cada programa cumpre com rigor os requisitos exigidos pelo mercado de trabalho. Importa salientar que a nossa formação beneficia de um amplo reconhecimento, não apenas no **espaço Europeu**, mas também no conjunto dos **países de língua oficial portuguesa** (CPLP).

Assim, ao escolher a Insignis West, o formando opta por uma instituição que garante uma certificação de prestígio e com validade internacional, essencial para a progressão e valorização de carreiras globais.

Certificações e Parcerias



Contatos

- **Insignis West – Lisboa – Portugal**

Alameda Roentgen, 4 – A- Escritório 6, 1600-759
+351 211 392 068 + 351 917 52
formacao@insigniswest.com

- **Insignis West – Luanda – Angola**

Condomínio Espaço Avenida, casa n.º 6, Porta 16
Av. Samora Machel, Luanda, Talatona
+244 946 159 308 Ou +244 933 976 087
luanda.office@insigniswest.com