INTEGER CONSULTING

Soluções de cibersegurança que todas as empresas devem considerar hoje

A sua organização está realmente preparada para as ameaças atuais? Uma cibersegurança robusta protege mais do que os sistemas. Ajuda a proteger o seu negócio, as suas pessoas e a confiança que conquistou junto dos seus clientes.

OS NÚMEROS

389%
de aumento anual do número de vítimas de ransomware (com contribuição do cibercrime suportado por IA).
Fonte

97%
das organizações reportam incidentes de segurança relacionados com IA devido à ausência de controlos de acesso adequados.
Fonte

62%
das violações de dados envolvem erro humano.
Fonte

43%
das empresas europeias afirmam não dispor das pessoas e competências para atingir os objetivos de cibersegurança.
Fonte

241
dias é o tempo médio para identificar e conter uma violação de dados.
Fonte

$4.4M
é o custo médio global de uma violação de dados.
Fonte

A boa notícia?
Estes riscos podem ser significativamente reduzidos com a abordagem e capacidades adequadas.

OS 6 PILARES DE UMA ESTRATÉGIA SÓLIDA DE CIBERSEGURANÇA

1 Planeamento e Avaliação de Risco
Não pode proteger o que não conhece.

- **Avaliação de riscos de segurança** — Identificar vulnerabilidades mais críticas.
- **Análise da maturidade em segurança** — Perceber onde está e onde melhorar.
- **Avaliação dos riscos associados à IA** — Compreender impacto na postura de segurança.
- **Roadmap de cibersegurança** — Definir plano prático para resiliência a longo prazo.

Ganhe visibilidade antes de investir em tecnologia.

2 Monitorização Contínua
Quanto mais rápido detetar uma ameaça, menor será o seu impacto.

- **SOC 24/7** — Manter sistemas críticos sob vigilância.
- **SIEM** — Centralizar e analisar eventos de segurança.
- **EDR/XDR** — Detetar e responder a ameaças nos endpoints.
- **Gestão de vulnerabilidades** — Identificar e priorizar fragilidades.
- **Gestão de firewalls** — Reforçar primeira linha de defesa.

As ameaças cibernéticas não trabalham em horário de expediente.

3 Testes de Segurança
Descubra vulnerabilidades antes dos atacantes.

- **Testes de intrusão (Pentest)** — Simular ataques reais aos sistemas.
- **Exercícios Red Team** — Desafiar as capacidades de defesa.
- **Simulações de phishing** — Preparar a equipa para ataques de engenharia social.
- **Testes de segurança física** — Avaliar riscos para além do ambiente digital.

Valide se os seus controlos funcionam em cenários reais.

4 Infraestruturas e Aplicações Seguras
A segurança funciona melhor quando faz parte da conceção e não quando é acrescentada no final.

- **Arquiteturas cloud seguras** — Proteger ambientes cloud desde o primeiro dia.
- **DevSecOps** — Integrar segurança ao longo do ciclo de desenvolvimento.
- **Revisão segura do código** — Eliminar vulnerabilidades antes da entrada em produção.
- **Proteção IoT/OT** — Proteger equipamentos ligados e ambientes industriais.
- **Prevenção da perda de dados** — Proteger informação crítica para o negócio.
- **Hardening de sistemas** — Reduzir superfícies de ataque desnecessárias.

Integre a segurança desde o início, em vez de corrigir problemas mais tarde.

5 Resposta a Incidentes e Continuidade do Negócio
Não é uma questão de "se", mas de "quando".

- **Resposta a incidentes** — Conter ameaças e minimizar interrupções.
- **Proteção contra ransomware** — Proteger ativos críticos face a ataques.
- **Backups seguros** — Salvaguardar informação essencial.
- **Continuidade do negócio** — Garantir o funcionamento das operações essenciais.
- **Recuperação de desastres** — Restabelecer rapidamente após incidentes.

Cada hora ganha reduz o impacto financeiro.

6 Conformidade e Governação
A conformidade deve fortalecer o negócio, não aumentar a complexidade.

NIS2 & DL português 125/2025 | RGPD | ISO 27001 | PCI-DSS | CIS Controls

Uma boa governação melhora a resiliência e facilita o cumprimento dos requisitos regulamentares.

A IA ESTÁ A TRANSFORMAR A CIBERSEGURANÇA

Os atacantes usam IA, os defensores também devem fazê-lo. A IA ajuda a:

- Detetar ameaças mais rápido
- Automatizar tarefas repetitivas
- Melhorar resposta a incidentes
- Reforçar operações de segurança

Mas a tecnologia por si só não é suficiente, a experiência humana continua a sua melhor defesa.

PERGUNTE-SE...

- Conhecemos os principais riscos de cibersegurança?
- Somos capazes de detetar um ataque na hora?
- Os colaboradores estão preparados para tentativas de phishing?
- A infraestrutura é testada regularmente?
- Conseguimos cumprir os requisitos regulamentares?

Se respondeu "não" a alguma, este é o momento certo para reforçar a maturidade da sua organização.

A CIBERSEGURANÇA É UM COMPROMISSO CONTÍNUO

Na Integer, combinamos conhecimento especializado, metodologias comprovadas e as tecnologias certas para ajudar a reduzir riscos, reforçar a resiliência e antecipar ameaças em constante evolução.

Juntos, vamos construir uma organização mais resiliente?

integerconsulting.pt