



Parceiro de Confiança

AUDITORIA

Serviços de Auditoria – Tem como objectivo último dotar uma organização com informação de valor sobre a sua conformidade face a práticas pré-seleccionadas;

AUDITORIA	Decreto-Lei 25/2004	Credenciação de entidades certificadoras emitentes de certificados digitais qualificados
	Portaria 701-G:2008	Credenciação de Plataformas Públicas Electrónicas
	ISO 27001 Audit	Certificação internacional em Gestão da Segurança da Informação (3rd Party Audit)
		Auditoria Interna de Segurança da Informação (área física, lógica e processual) (2nd Party Audit)
	ISO 25999 Audit	Certificação internacional em Gestão da Continuidade do Negócio (3rd Party Audit)
		Auditoria Interna ao modelo de gestão de continuidade de negócio (2nd Party Audit)
ISO 20000 Audit	Certificação internacional em Gestão de Serviços de SI/TI (3rd Party Audit)	
	Auditoria interna aos processos de gestão de serviços de SI/TI (2nd Party Audit)	

Benefícios-chave

- A disponibilidade de informação credível, isenta e de valor sobre o estado actual da organização, no âmbito auditado;
- O acesso a relatórios detalhados com propostas para acções de mitigação de não conformidade, baseadas em boas práticas reconhecidas;
- O acesso a relatórios com recomendações indexadas quanto a níveis de risco apercebido resultantes da aplicação de metodologia reconhecida;
- A possibilidade de acesso a uma ferramenta de auxílio à execução regular de auditorias internas a âmbitos pré-seleccionados;
- A execução de serviços reconhecidos para credenciação internacional.



Serviço de Auditoria CPD Assessment

Um dos serviços prestados no âmbito da Auditoria é o *CPD Assessment*, que avalia os riscos de segurança de um Centro de Processamento de Dados a partir das análises de activos não tecnológicos (ambientes físicos, pessoas e processos). O objectivo é a avaliação dos riscos do ambiente do CPD em matéria de segurança e conformidade proporcionando um melhor direccionamento do investimento em iniciativas de mitigação, através de recomendações, prioritizadas de acordo com a gravidade dos riscos/não-conformidades encontradas. Por exemplo:

- Controlo de acessos (Access Control)
- Estrutura do edifício/ambiente (Building Infrastructure)
- Cablagem (Cabling)
- Controlo climático (Climate control)
- Conformidade de Servidores (Compliance)
- Comunicações dados/voz (Data/Voice communication)
- Circuitos eléctricos (Electric Circuits and Power)
- Protecção e combate a incêndios (Fire protection and Treatment)
- Hidráulica (Hydraulics)
- Identificação e autenticação (Identification and Authentication)
- Abate de Informação (Information disposal)
- Incidentes de segurança (Security Incidents)
- Ambiente de Trabalho (Work Environment)

No final, a Prológica apresenta um Inventário do ambiente analisado, um Relatório de Análise de Riscos (RAR), um ScoreCard – Painel de Controlo (visão executiva dos riscos no ambiente auditado) e realiza um Workshop de apresentação de resultados.

