

Segurança da Informação

ISO 27001 - SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO



www.paralleldiscover.pt





A ISO 27001 é uma norma internacional publicada pela International Standardization Organization (ISO) e descreve como gerenciar a segurança da informação em uma organização. A versão mais recente desta norma foi publicada em 2013, e seu título completo agora é ISO/IEC 27001:2013. A primeira versão desta norma foi publicada em 2005, e foi desenvolvida com base na Norma Britânica BS 7799-2.





**Mantenha seguros
seus dados e as
informações de seus
clientes.**

Segurança da Informação

Nos últimos anos as tecnologias de informação e comunicação têm evoluído de forma rápida, fazendo com que as organizações tenham maior eficiência e rapidez nas tomadas de decisão, devido a este fato as chances de uma empresa não usar sistemas de informação tornou-se praticamente nula. Neste contexto a importância de se utilizar mecanismos de segurança e de armazenamento das informações é vital para a sobrevivência e competitividade destas organizações.

A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para a implementação da gestão da segurança da informação em uma organização. Ela também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou que uma organização implementou a segurança da informação em conformidade com a ISO 27001.

Ao longo dos anos, milhares de profissionais contribuíram com o seu know-how e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos.

A norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objectivo de mitigarem e gerirem adequadamente o risco da organização.

O foco da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade da informação

de uma organização. Isto é feito identificando-se quais potenciais problemas podem ocorrer com a informação (i.e. avaliação de risco), e então definindo quais necessidades devem ser atendidas para prevenir tais problemas de ocorrerem (i.e. mitigação de risco ou tratamento de risco).

A principal filosofia da ISO 27001 é baseada na gestão de riscos: descobrir onde os riscos estão, e então trata-los sistematicamente





Segurança da informação é a proteção da informação de vários tipos

de ameaças para garantir a continuidade do negócio, minimizar o risco ao 16 negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Aplicar a Segurança da Informação não é mais um modismo, hoje se refere a uma necessidade estabelecida por normas e padrões técnicos.



12



Os benefícios

Existem 4 benefícios de negócio essenciais que uma organização pode atingir com a implementação desta norma de segurança da informação

CONFORMIDADE COM REQUISITOS LEGAIS – existem cada vez mais leis, regulamentações e requisitos contratuais relacionados a segurança da informação, e a boa notícia é que muitos deles podem ser resolvidos pela implementação da ISO 27001 – esta norma dá uma metodologia perfeita para estar em conformidade com todos estes requisitos.

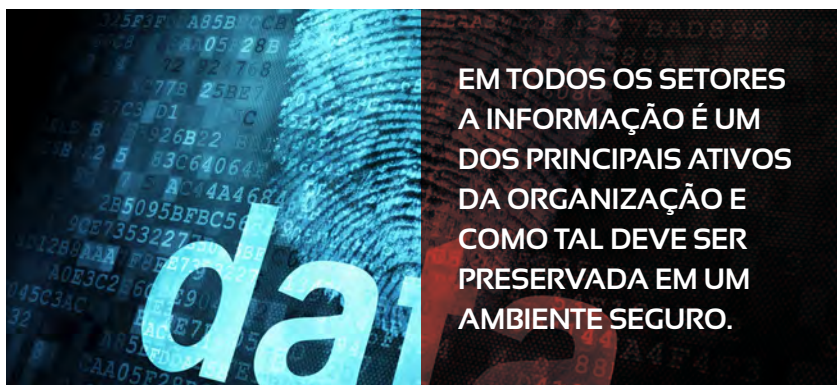
OBTER VANTAGEM DE MARKETING – se sua organização

obtem a certificação e seus competidores não, você pode ter vantagem sobre eles na visão de clientes que são sensíveis a questão de manter suas informações seguras.

REDUZIR CUSTOS – a principal filosofia da ISO 27001 é prevenir incidentes de segurança de ocorrerem; e cada incidente, sendo este grande ou pequeno custa dinheiro – desta forma, ao prevenir incidentes sua organização

economizará uma quantidade significativa de dinheiro. E a melhor coisa de tudo – investimento na ISO 27001 é muito menor do que a economia em custo que você obterá.

MELHOR ORGANIZAÇÃO – tipicamente, organizações que crescem rápido não tem tempo para fazer uma pausa e definir seus processos e procedimentos – e como uma consequência, muito frequentemente os empregados não sabem o que precisa ser feito, quando e por quem. A implementação da ISO 27001 ajuda a resolver tal situação porque ela encoraja as organizações a escrever seus principais processos (mesmo aqueles que não são relacionados a segurança), possibilitando a elas reduzir a perda de tempo de seus empregados.



O PROCESSO DE CERTIFICAÇÃO

A certificação é efectuada em várias etapas.



Construção da proposta da Parallel Discover.

Construção da proposta da Parallel Discover. Realização da auditoria prévia (opcional), onde são identificados os pontos fortes e pontos de melhoria.



Auditoria de concessão

Auditoria de concessão 1ª fase – Análise dos documentos do Sistema de Gestão da Segurança da Informação e outros pontos-chave. É emitido um relatório com as constatações. 2ª fase – Entrevistas aos colaboradores, verificação de registos e observação das práticas de trabalho. É emitido um relatório com as constatações e um certificado se a decisão for favorável.



Auditorias de acompanhamento

Verificação do Sistema de Gestão da Segurança da Informação e da implementação do plano com as ações de melhorias.



Auditoria de renovação

Após 3 anos da auditoria de concessão.



Contacta-nos

PARALLEL DISCOVER Lda.

Urbanização das Palmeiras lote 6, loja A
8400-623, Parchal
Algarve, Portugal
Email: info@paralleldiscover.pt

www.paralleldiscover.pt

