# PERGUNTAS MAIS FREQUENTES CERTIFICAÇÃO NBR ISO/IEC 27001

Através da vasta experiência, adquirida ao longo dos últimos anos, atuando em Certificações de Sistemas de Gestão, a Fundação Vanzolini vem catalogando as principais dúvidas dos clientes relacionadas às respectivas normas, suas características e o processo de certificação.
Esperamos que a lista abaixo possa elucidar suas dúvidas.

**1. O que é segurança da informação?**
Segundo a norma NBR ISO/IEC 17799:2005, segurança da informação é a proteção da informação contra vários tipos de ameaças de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno sobre investimentos e oportunidades de negócios. Ainda segundo a NBR ISO/IEC 17799:2005 a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

**2. O que é a NBR ISO IEC 27001:2006?**
É a norma de certificação para Sistemas de Gestão da Segurança da Informação, editada em português em abril de 2006 e que substituiu a BS 7799-2. Esta norma foi preparada para prover um modelo para o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação.
A NBR ISO IEC 27001 e NBR ISO IEC 17799 foram o par consistente de normas relativas a Sistema de Gestão de Segurança da Informação.

**3. O que é NBR ISO/IEC 17799?**
A A NBR ISO/IEC 17799 é a versão brasileira da norma ISO homologada pela ABNT, a versão válida é de 2005. É o Código de Prática para Gestão da Segurança da Informação. Serve como referência para a criação e implementação de práticas de segurança reconhecidas internacionalmente, incluindo: Políticas, Diretrizes, Procedimentos, Controles
È um conjunto completo de recomendações para: Gestão da Segurança de Informação e Controles e práticas para a Segurança da Informação.
Atenção: a norma de certificação é a **NBR ISO IEC 27001:2006,** a NBR ISO IEC 17799 é somente uma norma de referência contida na norma de certificação.

**4. Qual é a importância que as organizações dão hoje a ISO 27001?**
Todas as grandes organizações do mundo, sejam públicas ou privadas, já tomaram conhecimento sobre as normas ISO. Diversas pesquisas demonstram que muitas dessas organizações já estão incorporando os controles das normas em suas políticas de segurança.

**5. Qual é a importância da ISO 27001?**
Ela permite que uma empresa construa de forma muito rápida uma política de segurança baseada em controles de segurança eficientes. Os outros caminhos para se fazer o mesmo, sem a norma, são constituir uma equipe para pesquisar o assunto ou contratar uma consultoria para realizar essa tarefas.

**6. Essas normas se aplicam a qualquer tipo de organização?**
As normas foram criadas e se adaptam bem a organizações comerciais. Instituições de ensino, instituições públicas e outras assemelhadas podem ter dificuldades em implantar certos controles da norma devido a seus ambientes serem diferentes dos de uma empresa comercial. Apesar disso, qualquer organização pode aproveitar grande parte dos controles da norma para implementar segurança da informação em suas instalações.

**7. O que é SGSI?**
Sistema de Gestão de Segurança da Informação é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para segurança da informação. Uma empresa que implante a norma ISO 27001 acaba por constituir um SGSI.

**8. Quais são as etapas para se constituir um SGSI?**
Em primeiro lugar, deve-se definir quais são seus limites (sua abrangência física, lógica e pessoal). Depois devem ser relacionados os recursos que serão protegidos. Em seguida relaciona-se quais são as possíveis ameaças a esses recursos, quais são as vulneráveis a que eles estão submetidos e qual seria o impacto da materizalização dessas ameaças. Por fim,com base nessas informações, são priorizados os controles necessários para garantir a segurança desses recursos.

**9. Para implantar a norma em uma empresa é obrigatório empregar todos os seus controles?**
Não. Aplicam-se somente os controles para os serviços, facilidades, espaços e condições existentes na empresa. Por exemplo, se a empresa não tem acesso remoto de usuários, todos os controles referentes a esse tipo de acesso podem ser ignorados.

**10. O que é a Declaração de Aplicabilidade?**
É um documento exigido pela NBR ISO IEC 27001 no qual a empresa tem que relacionar quais controles do Anexo A são aplicáveis e justificar os que não são aplicáveis ao seu SGSI.

**11. Como obter a norma NBR ISO IEC 27001?**
As normas NBR ISO, assim como as de outros países, têm direitos autorais. As normas da série NBR ISO devem ser adquiridas na ABNT – Associação Brasileira de Normas Técnicas.

**12. Como a ISO 27001 se relaciona com as normas ISO 9000 e ISO 14000?**
A ISO 27001 harmoniza-se com essas normas na medida que segue a suas estruturas e conteúdos. A 27001 inclui um PDCA semelhante aos existentes na ISO 9001 e ISO 14000 com objetivo de estabelecer um contínua gestão da segurança da informação.

**13. O que é PDCA?**
PDCA (*Plan-Do-Check-Act* ou Planejar-Executar-Verificar-Agir) é um método de gestão que se carateriza por um ciclo de ações que se repete continuamente de forma a incorporar alterações no ambiente. Nas normas de gestão acima mencionadas é empregado para garantir uma efetiva gestão da empresa.

**14. Existe legislação que obrigue o uso da ISO 27001?**
As leis variam de país para país. A rigor não existem leis que obriguem o emprego de tais normas. No Brasil, existem recomendações no sentido de empregar-se a norma emitidas por entidades como a Fenabam, o Conselho Federal de Medicina, a ICP-Brasil, dentre outros. No Reino Unido, a Data Protection Act promulgada em 1998 e, nos Estados Unidos, a lei Sarbanes-Oxley (que atinge subsidiárias de empresas americanas de capital aberto instaladas no Brasil), promulgada em 2002, determinam cuidados no trato das informações que, na prática, obrigam as empresas a empregar a ISO 27001/ISO 17799 como uma forma de demonstrarem que estão procurando cumprir os requisitos de segurança determinados por essas leis.

**15. O que é certificação?**
A certificação é um documento emitido por uma entidade certificadora independente que garante que uma dada empresa implantou corretamente todos os controles da norma aplicáveis. A certificação é emitida após uma auditoria externa para verificação da conformidade da empresa com a norma.

**16. Para que serve a certificação?**
Ela comprova, para as empresas certificadas, que a segurança da informação está garantida de forma efetiva, o que não significa, contudo, que a empresa esteja imune a violações de segurança. Além disso, a certificação comprova, para os clientes e fornecedores da empresa, o a preocupação que esta tem com a segurança da informação, reforçando sua imagem junto ao mercado. Dependendo da atividade da empresa, essa certificação pode ser essencial para a realização de certos negócios.

**17. Pode-se aplicar a ISO 27001 e realizar apenas uma auditoria interna?**
Sim. Na realidade, a maior parte das empresas a emprega dessa forma, uma vez que elas ainda não identificaram a necessidade ou a possibilidade de realizarem o processo de certificação.

**18. Qual é o custo de uma certificação?**
O custo depende de vários fatores, tal como quanto tempo o responsável pela certificação necessita para avaliar a conformidade da empresa com relação à norma, o tamanho e a complexidade da empresa e de seus sistemas.

**19. Muitas empresas já obtiveram a certificação?**
Até o final de 2004, mais de 2017 empresas em todo mundo receberam a certificação BS7799-2 a certificação NBR ISO 27001:2005 até o presente momento somente 1 empresa obteve no mundo, e esta empresa foi no Brasil, Módulo Security.
Informações atualizadas podem ser obtidas no site www.xisec.com

**20. Quantas e quais empresas foram certificadas no Brasil?**
Cinco empresas brasileiras obtiveram a certificação até 2004: Módulo Security, Banco Matone, Serasa, Samarco Mineração e Unisys. Sendo que a Módulo já fez a transição para a NBR ISO IEC 27001. Informações atualizadas sobre empresas certificadas no Brasil e no mundo podem ser obtidas no site www.xisec.com.

**21. Quem concede o certificado?**
Os certificados são emitidos por entidades certificadoras acreditadas por órgãos de credenciamento nacionais ou internacionais após realização de auditorias.

**22. Como são feitas estas auditorias?**
A auditoria do Sistema de Gestão da Segurança da Informação é dividida em 2 etapas: Auditoria de Documentação, conhecida como Fase 1 e Auditoria de Certificação, conhecida como Fase 2. Podendo existir também a Pré-Auditoria, esta por sua vez é opcional.

**23. O que é Auditoria de Documentação?**
Em razão do tema abordado esta norma envolve documentos e informações, muitas vezes, confidenciais, desta forma, fazem-se necessário uma análise prévia destes nas instalações da própria empresa visando à verificação de sua adequação e a segurança dos dados.
A Auditoria de Documentação é o primeiro contato com a equipe auditora.

**24. Qual a diferença entre a Auditoria de Documentação e a Pré-auditoria?**
A Auditoria de Documentação tem como foco a seguinte documentação: Declaração de Aplicabilidade, Relatório de Avaliação de Riscos e Análise Crítica pela Direção entre outros possíveis documentos associados a estes, conforme aplicável. Esta análise não contempla procedimentos e práticas específicos, uma vez que estes são objeto da Pré-auditoria, que tem por objetivo a análise crítica da adequação do sistema à norma.

**25. Pré-auditoria é o mesmo que Auditoria de Pré-certificação?**
Sim. Os dois termos são usados e reconhecidos pelo mercado para identificar um mesmo tipo de auditoria.

**26. Quando devo solicitar a Pré-auditoria?**
Após a implantação do Sistema de Gestão da Segurança da Informação e após ter realizado pelo menos um ciclo de auditoria interna e pelo menos uma análise crítica pela direção a empresa pode solicitar a realização da Pré-auditoria para verificar o nível de adequação à norma em questão.

**27. Minha empresa já possui a certificação pela norma anterior. Também posso solicitar uma Pré-auditoria segundo a nova versão?**
As empresas já certificadas podem solicitar a realização da Pré-auditoria para verificar o nível de adequação à norma em questão, após a adequação do Sistema de Gestão da Segurança da Informação e após ter realizado pelo menos um ciclo de auditoria interna . A FCAV recomenda que tenha também pelo menos uma análise crítica do sistema já com a nova estrutura.

**28. Para que serve a Pré-auditoria?**
A Pré-auditoria tem como principal objetivo a detecção de eventuais problemas conceituais que possam vir a ser despercebidos pela empresa em processo de certificação. Seria um exemplo de problema conceitual, a não aplicação de um requisito ou controle que influencie na Segurança da Informação da empresa. Isto pode ocorrer em razão de uma incorreta interpretação da norma para o negócio da empresa e/ou escopo considerado(s). No entanto, nestes casos a certificação não pode ser recomendada, causando transtornos para a empresa e uma certa decepção para todos os envolvidos.
A fim de reduzir os riscos de não certificação por problemas de adequação, os organismos certificadores em todo o mundo passaram a realizar análises prévias, estas análises prévias são chamadas de pré-auditoria.

**29. Como é feita a pré-auditoria?**
A Pré-auditoria é realizada nas instalações da empresa e segue os mesmos passos da Auditoria de Certificação: Reunião de Abertura, investigação, relato das não-conformidades e reunião de encerramento. Geralmente a equipe auditora da Pré-auditoria será a mesma da Análise Documental e da Auditoria de Certificação.
São verificados os procedimentos e a documentação em relação à sua adequação à norma de referência. O tempo dimensionado para esta auditoria, normalmente não permite que a equipe auditora tenha tempo para verificar se as práticas descritas na documentação estão adequadamente implementadas – isto é o que chamamos de auditoria de conformidade, que será realizada durante a Auditoria de Certificação (Inicial) e nas Auditorias de Manutenção (Anuais ou semestrais).

**30. No meu orçamento consta uma Pré-auditoria de um dia. Posso solicitar mais um ou dois dias?**
Sim. A carga horária definida no orçamento é mínima para checar todos os itens da norma. No entanto, caso a empresa deseje uma análise mais aprofundada, a carga horária poderá ser aumentada sem problema algum. Haverá um aumento proporcional no preço do evento.

**31. Posso pular a Pré-auditoria e ir direto para a Auditoria de Certificação?**
Sim. Tomando-se como base a experiência adquirida ao longo do tempo em certificações de sistemas de gestão, a FCAV recomenda fortemente a realização da Pré-auditoria, no entanto, se a empresa tem muita segurança na adequação e conformidade do seu sistema de gestão não há problema algum em ir direto para a Auditoria de Certificação.

**32. Se o auditor não encontrar problemas na Pré-auditoria posso já receber o certificado?**
Não. A Pré-auditoria tem objetivo distinto da Auditoria de Certificação. A Pré-auditoria verifica a adequação do sistema, não colhendo evidências suficientes de que as práticas refletem o

planejamento contido nos procedimentos. A verificação da implementação é feita na Auditoria de Certificação que não pode ser dispensada em nenhum caso.

**33. Qual é o prazo entre a Auditoria de Documentação e as Auditorias de Pré-certificação, Certificação e Manutenção?**
Com exceção às Auditorias de Manutenção, que devem ocorrer no mínimo anualmente, não há um prazo expressamente definido para que estes eventos ocorram, e os mesmos podem ser discutidos e acordados, conforme as necessidades de cada empresa. No entanto, a FCAV recomenda que a Auditoria de Documentação ocorra pelo menos 30 dias antes da Auditoria de Certificação e, caso seja solicitada, 30 dias antes da Pré-auditoria.

**34. Quem faz parte da equipe auditora?**
Normalmente, a equipe auditora é formada por um ou dois auditores com experiência em auditoria e conhecimentos do segmento de negócio da empresa. Por se tratar de uma norma específica, as auditorias do Sistema de Gestão de Segurança da Informação devem contar sempre auditores que detenham conhecimentos técnicos suficientes para compreender a linguagem dos auditados.

**35. A FCAV mantém cursos sobre esta norma?**
A FCAV mantém cursos abertos e “in company” para implementação do Sistema de Gestão da Segurança da Informação, formação de Auditores Internos do SGSI e formação de Auditores Líderes NBR ISO/IEC 27001.

**36. No caso de dúvidas, a quem devo consultar?**
Caso algumas dúvidas ainda permaneçam ou não tenham sido abordadas acima, não hesite em nos contatar pelo telefone (11) 3836-6566 ramais 103 ou 105.
Consulte também nossa home page: www.vanzolini.org.br