Normativos e Referenciais

Prof. Edson Pedro Ferlin

- Objetivos
  - Apresentar os normativos e referenciais de Segurança da Informação.
- Conteúdos
  - Normas nacionais e internacionais
  - Referenciais nacionais e internacionais
  - Certificação

SEGURANÇA DA INFORMAÇÃO

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação.

NORMA NBR ISO/IEC 27000

A série ISO 27000 constitui um padrão de certificação de sistemas de gestão promovido pelo *International Organization for Standardization* (ISO).

NORMA NBR ISO/IEC 27000

ISO 27001	•Requisitos para um sistema de gestão de Segurança da Informação
ISO 27002	•Boas práticas para a gestão de Segurança da Informação
ISO 27003	•Guia para a implantação de um sistema de gestão de Segurança da Informação (metodologia)
ISO 27004	•Define métricas e meios de medição para avaliar a eficácia de um sistema de gestão de Segurança da Informação
ISO 27005	•Fornece as diretrizes para o processo de gestão de risco de Segurança da Informação

ISO 27001 – Requisitos

A norma 27001 apresenta alguns requisitos que sugerem alguns procedimentos para uma boa Gestão de Segurança da Informação.

ISO 27002 – Código de Práticas

A norma ISO 27002 a partir de Julho de 2007 é o novo nome da norma ISO 17799.

Esta norma é um guia de boas práticas que descreve os objetivos de controle e os controles recomendados para a Segurança da Informação.

ISO 27003 – Guia de Implementação

A norma ISO 27003 aborda algumas diretrizes para a implementação de SGSI (Sistemas de Gestão de Segurança da Informação) e contem informações sobre como usar o modelo PDCA (*Plan-Do-Check-Act*) e os requisitos das suas diferentes fases, ou seja, fornecerá uma abordagem de processos orientada para o sucesso da implementação de um SGSI de acordo com a norma ISO 27001.

ISO 27004 – Métricas e Medição

A norma ISO 27004 especifica métricas e técnicas de medição aplicáveis para determinar a eficácia do SGSI (Sistema de Gestão de Segurança da Informação), os objetivos de controlo e os controles usados para implementar e gerir a Segurança da Informação. Estas métricas são usadas principalmente para medir os componentes da fase "CHECK" do ciclo PDCA (*Plan-Do-Check-Act*).

ISO 27005 – Diretrizes de Gestão de Risco

A norma ISO 27005 estabelece diretrizes para a gestão de risco em Segurança da Informação, fornecendo indicações para implementação, monitoramento e melhoria contínua do sistema de controles.

É aplicada a todos os tipos de organizações que se destinam a gerir os riscos que possam comprometer a segurança das suas informações.

ISO 27006 – Diretrizes de Serviços de Recuperação de Desastres

A norma ISO 27006 especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um SGSI (Sistema de Gestão de Segurança da Informação).

CERTIFICAÇÃO

A certificação é uma declaração formal que exprime a veracidade de determinado contexto.

É emitida por uma organização certificadora, organização essa que tem credibilidade e autoridade moral e legal.

Processo de Certificação

A certificação segue a avaliação de um determinado processo, sistema ou produto segundo normas e critérios que visa verificar o cumprimento dos requisitos, conferindo um certificado com o direito de uso de uma marca de conformidade associada ao produto ou imagem institucional se os requisitos estiverem plenamente atendidos.

Validade da Certificação

A certificação de uma organização é temporária, todas as normas são reavaliadas periodicamente por decisão do organismo internacional de normalização e responsável pela publicação da maior parte dos referenciais normativos reconhecidos internacionalmente (ISO).

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) ProfEdsonPedroFerlin