Auditoria de Sistemas

Prof. Luiz Antonio

AULA 07

Modelos para segurança da informação

Introdução aos modelos de segurança da informação

Estrutura do modelo ISO/IEC 27001

Estrutura do modelo ISO/IEC 27002

Introdução aos modelos de segurança da informação

A crescente utilização de soluções informatizadas nas diversas áreas de serviços exige níveis de segurança adequados e maior exposição dos valores e informações. A evolução da tecnologia de informação, migrando de um ambiente centralizado para um ambiente distribuído, interligando redes internas e externas, somada à revolução da Internet, mudou a forma de se fazer negócios.

Isto fez com que as empresas se preocupassem mais com o controle de acesso às suas informações bem como a proteção dos ataques, tanto internos quanto externos. Paralelamente, os sistemas de informação também adquiriram grande importância para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

A segurança da informação tem como característica principal tentar preservar a disponibilidade, a integridade e o caráter confidencial da informação.

O **comprometimento do sistema de informações**, por problemas de segurança, pode causar grandes prejuízos à organização. Diversos tipos de incidentes podem ocorrer a qualquer momento, podendo atingir a informação confidencial, a integridade e disponibilidade.

Introdução aos modelos de segurança da informação

Problemas de **quebra de confidência**, por vazamento ou roubo de informações sigilosas, podem expor para o mercado ou concorrência as estratégias ou tecnologias da organização, eliminando um diferencial competitivo, comprometendo a sua eficácia, podendo perder mercado e até mesmo ir à falência.

Problemas de disponibilidade podem ter um impacto direto sobre o faturamento, pois deixar uma organização sem matéria-prima ou sem suprimentos importantes ou mesmo, o impedimento de honrar compromissos com clientes, prejudicam sua imagem perante os clientes, gerando problemas com custos e levando a margem de lucro a ficar bem comprometida.

Problemas de integridade, causados por invasão ou fatores técnicos em dados sensíveis, sem uma imediata percepção, irão impactar sobre as tomadas de decisões. Decisões erradas fatalmente reduzirão o faturamento ou aumentarão os custos, afetando novamente a margem de lucros.

A invasão da página de Internet de uma empresa, com modificação de conteúdo, ou até mesmo a indisponibilidade de serviços on-line, revela a negligência com a segurança da informação e causa perdas financeiras a quem sofreu algum tipo de ataque.

Introdução aos modelos de segurança da informação

Normas ISO

Uma vez que a segurança da informação busca garantir a confidencialidade, a integridade e a disponibilidade das informações, o emprego de um conjunto de boas práticas torna-se fundamental neste desafio. Neste sentido, as normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação, tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. São relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. Mas estas não são as únicas relacionadas à segurança da informação e cibersegurança.

Estrutura do modelo ISO/IEC 27001

A norma ABNT NBR ISO/IEC 27001:2013 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo.

Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização, incluindo, ainda, requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

A ABNT NBR ISO/IEC 27001 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Estrutura do modelo ISO/IEC 27001

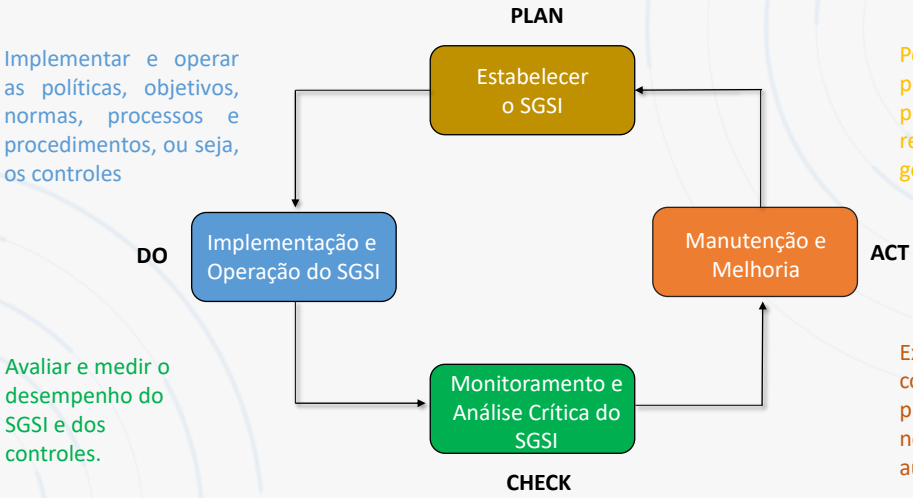
Esta norma recomenda a análise crítica e entendimento do contexto da empresa, envolvendo as questões internas e externas que são relevantes para seu propósito; a compreensão das necessidades e expectativas das partes interessadas; e o escopo do sistema de gestão de segurança da informação.

No aspecto de liderança, é fundamental que a Alta Direção demonstre sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação por vários meios, que estabeleça uma política de segurança da informação (PSI) e que assegure que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

As ações para contemplar riscos e oportunidades devem ser estabelecidas pela organização com foco na avaliação e tratamento de riscos de segurança da informação. Complementarmente, a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação a partir da definição de competências, adoção de programas de conscientização, comunicação e documentação das ações.

Na implementação do SGSI é recomendável a adoção do ciclo PDCA (método interativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos). As 4 (quatro) etapas do respectivo ciclo envolvem: *Plan* (planejar), *Do* (executar), *Check* (verificar) e *Act* (agir). Este ciclo considera, no contexto do SGSI, um conjunto de atividades conforme pode ser verificado na figura a seguir.

Estrutura do modelo ISO/IEC 27001



Estrutura do modelo ISO/IEC 27002

Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Esta Norma é projetada para ser usada por organizações que pretendam:

a) Selecionar controles dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001;
b) Implementar controles de segurança da informação comumente aceitos;
c) Desenvolver seus próprios princípios de gestão da segurança da informação.

Esta Norma contém 14 seções de controles de segurança da informação de um total de 35 objetivos de controles (declarações do que se espera que seja alcançado) e 114 controles (declarações específicas do controle, para atender ao objetivo de controle).

Estrutura do modelo ISO/IEC 27002

As 14 seções de controles de segurança da informação estão distribuídas da seguinte forma:

1	Política de Segurança da Informação	6	Criptografia	11	Relacionamento na Cadeia de Suprimentos
2	Organização da Segurança da Informação	7	Segurança Física e do Ambiente	12	Gestão de Incidentes de Segurança da Informação
3	Segurança em Recursos Humanos	8	Segurança nas Operação	13	Aspectos de SI na Gestão da Continuidade de Negócios
4	Gestão de ativos	9	Segurança nas Comunicações	14	Conformidades
5	Controle de Acesso	10	Aquisição, Desenvolvimento e Manutenção de Sistemas		