Capítulo 2

Família de normas ISO/IEC 27000

Neste capítulo apresentamos as normas da família ISO/IEC 27000, que tem como principal objetivo orientar o Sistema de Gestão de Segurança da Informação. As normas mais conhecidas são as ISO 27001 e ISO 27002, que estão relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico.

É de fundamental importância entender o motivo de sua criação e o porquê das organizações seguirem essas normas, pois uma área de TI que despreza essas regras estará sujeita à vulnerabilidade de seus ativos de TI e consequentemente à perda deste patrimônio.

1 ISO 27000 – Gestão da Segurança da Informação

A norma ISO/IEC 27000 é um conjunto de padrões internacionais desenvolvidos para o controle de qualidade e segue as normas ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que fornecem uma estrutura para gerenciamento de segurança da informação útil para toda e qualquer organização que deseja implementá-la, pública ou privada, grande ou pequena.

Elas tratam exclusivamente sobre o Sistema de Gestão de Segurança da Informação (SGSI), sendo as normas mais conhecidas a ISO 27001 e a ISO 27002.

Estão relacionadas à segurança de dados digitais e dos sistemas de armazenamento eletrônico de dados. É uma regra de segurança que é aplicada para todos os tipos de dados e informações de um determinado sistema e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade.

A série de normas da ISO 27000 possui diversos segmentos, e cada um deles possui uma função específica, mas todos estão diretamente relacionados a criação, manutenção, melhoria, revisão, funcionamento e análise de um SGSI. As normas podem ser adotadas independentemente do tamanho ou tipo da empresa, e suas diretrizes buscam fazer com que não só as informações da organização, mas principalmente os sistemas ofereçam segurança aos usuários.

1.1 Principais normas da família ISO/IEC 27000

A família ISO/IEC 27000 é bem extensa e todas as suas normas estão relacionadas ao SGSI.

A ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação – é a única norma da família 27000 que é passível de certificação acreditada. Todas as demais são apenas guias de boas práticas.

A ISO/IEC 27002 fornece um guia completo para a implementação do SGSI, que deve ser escolhido com base em uma avaliação de riscos dos ativos mais importantes da empresa. Ela pode ser utilizada para apoiar a implantação do SGSI em organizações de qualquer natureza. Os principais itens que compõe esta norma são:

- Gestão de ativos
- Segurança em recursos humanos
- Segurança física e do ambiente
- Segurança das operações e comunicações
- Controle de acesso
- Aquisição, desenvolvimento e manutenção de sistemas
- Gestão de incidentes de segurança da informação
- Gestão de continuidade do negócio
- Conformidade

A ISO/IEC 27003 é a norma técnica que objetiva fornecer orientações sobre os requisitos para a implantação de um Sistema de Gestão de Segurança da Informação (SGSI) conforme especificado na norma ISO/IEC 27001, além de sugerir algumas recomendações, possibilidades e permissões em relação a eles. O seu principal objetivo não é o de ditar as normas para o desenvolvimento do SGSI, mas sim fornecer um guia de boas práticas.

A ISO/IEC 27004 fornece diretrizes para o desenvolvimento e uso de métricas e medições a fim de avaliar a eficácia de um SGSI implantado

e de todos os controles ou grupos de controles, conforme especificado no sistema.

A ISO/IEC 27005 fornece as diretrizes para o gerenciamento dos riscos de segurança da informação (SI) e a base dos conceitos especificados na ISO 27001. Ela também pode auxiliar grandemente na implementação e certificação dos sistemas de gestão.

2 ISO 27001 – Fundamentos de segurança da informação

A ISO 27001 é uma norma que tem como objetivo a criação de um SGSI (Sistema Gestão de Segurança da Informação). Ele não sugere, exige, nem especifica as ações que devem ser adotadas de acordo com a realidade da empresa, mas inclui sugestões de documentação de processos e procedimentos, melhoria contínua, auditorias internas e ações corretivas e preventivas.

Sua implementação procura garantir um compromisso com a proteção da informação, que é uma das principais preocupações da atualidade, fornecendo às organizações um modelo de melhores práticas para identificar, analisar e, então, implementar controles para gerenciar riscos de segurança da informação e proteger a confidencialidade, integridade e disponibilidade de dados essenciais aos negócios.

Esta norma é a base de especificações e procedimentos tecnológicos que deu origem à LGPD (Lei Geral sobre a Proteção de Dados).

Seus principais objetivos são:

- Conseguir o apoio da direção da empresa e realizar o planejamento de todas as atividades necessárias para sua execução.
- Definir o escopo do SGSI.

- Definir as regras para a avaliação e tratamento de riscos.
- Definir o plano de tratamento de riscos.
- Definir como será mensurado o nível de eficácia dos controles.
- Implementar todos os controles necessários e procedimentos aplicáveis de acordo com a sua aplicabilidade.
- Implementar em toda a organização programas de treinamentos e conscientização.
- Executar as atividades diárias definidas pela documentação do Sistema de Gestão de Segurança da Informação.
- Monitorar e avaliar o Sistema de Gestão de Segurança da Informação.
- Realizar auditoria e análise crítica.
- Implementar ações preventivas e corretivas se for necessário.

2.1 Definição de informação e dado

A informação é um conjunto de dados que, quando alinhados e processados, conseguem constituir algo relevante. Quando os dados são tratados sob uma certa visão, eles podem transmitir uma mensagem de importância para quem estiver lendo e diminuir as incertezas ou até mesmo aperfeiçoar o conhecimento sobre determinado assunto.

O dado é um elemento que faz parte da matéria-prima de uma informação. Ele pode ser um número, um valor, uma medição e uma constatação.

Numa rápida explicação sobre dados e informações, podemos dizer que dado é um elemento que faz parte de uma informação. Ele, por si só, não tem um significado muito expressivo, mas quando associado a

outros dados consegue formar um sentido que constitui uma informação. Como exemplo, podemos analisar a seguinte situação:

NA PRÁTICA

Uma pesquisa (fictícia) sobre os engenheiros da cidade de São Paulo

Numa pesquisa sobre profissões, a palavra 'engenheiros' não possui um significado muito importante por ser apenas um dado. Mas quando é associada a uma especialidade, a um estado, a uma cidade, a um bairro, consegue transmitir uma informação relevante.

Segundo a nossa pesquisa, há na cidade de São Paulo 500 mil engenheiros, sendo 30% mecânicos, 32% civil, 28% eletricistas e 10% nas demais especialidades. Esta é uma informação muito importante em função dos dados coletados. A partir desta informação surge um terceiro fator, que é a produção do conhecimento.

Segundo Thomas A. Stewart "a informação e o conhecimento são as armas nucleares da nossa era" (STEWART, 1998, p. xiii).

2.2 Formas da informação

Informação são dados tratados. O resultado do processamento de dados são as informações. As informações possuem significado amplo e podem contribuir no processo de tomada de decisões. Elas se apresentam em diferentes tipos e formatos, a depender do nível funcional e dos contextos de decisão vivenciadas pelos gestores. A informação pode também revelar um conhecimento inscrito ou gravado sob uma forma escrita, oral ou audiovisual.

As informações em nível operacional são utilizadas em situações do dia a dia e são previsíveis e de efeito imediato, isto é, ocorrem, por exemplo, quando um determinado equipamento é substituído por apresentar em seu histórico altos níveis de manutenção. As informações de nível gerencial são tratadas de maneira analítica e sintética, combinando-se

diversas fontes e resultando em efeitos mais amplos e consolidados. As informações de nível estratégico são aquelas presentes em níveis acima dos gerenciais. Os executivos utilizam essas informações em situações complexas e incertas, mas ao analisar seu histórico ao longo de um período extenso conseguem antever as tendências de mercado, fazendo análises preditivas e, com isso, conseguem alterar a rota dos negócios e conquistar melhores posições no mercado.

2.3 Sistemas e tecnologia da informação

O sistema é um conjunto de elementos inter-relacionados com um objetivo: produzir relatórios que nortearão a tomada de decisões gerenciais. Neste percurso, pode-se identificar o processo que transforma dados em entrada, agregados aos comandos gerenciais, em saídas. Assim, o feedback do sistema faz com que, no meio da manutenção do ciclo operacional, sejam ativadas novas estratégias empresariais visando a geração de informações qualitativas ou quantitativas para suportar o alcance do sucesso absoluto (IMONIANA, 2012).

Um sistema possui três atividades básicas que produzem as necessidades de informação dentro da organização, que são:

- entrada
- processamento
- saída

No Brasil, a partir do início da década de 1970, os sistemas tinham como principal objetivo o processamento rápido das informações em função do volume, e suas funções eram, na sua maioria, de geração de relatórios analíticos e sintéticos. As informações ficavam armazenadas em fitas magnéticas, cartões perfurados e discos rígidos removíveis.

A partir do início da década de 1980, com o advento dos microcomputadores, os sistemas passaram por uma mudança radical de

paradigma, de descentralização de informações, novos conceitos de processamentos, diminuição substancial dos relatórios e utilização de terminais de consultas.

2.3.1 Tecnologia da informação – TI

A tecnologia da informação – TI (em inglês, information technology — IT) pode ser definida como o conjunto de atividades e soluções que utiliza a computação para a obtenção, o armazenamento, a proteção, o processamento, o acesso, o manuseio e o uso das informações para fins específicos.

É um conjunto de soluções que utiliza equipamentos (hardware) e os sistemas (softwares) para fazer o tratamento das informações. Ela é dividida de acordo com as seguintes áreas:

- programação;
- banco de dados;
- processamentos;
- suporte técnico;
- segurança da informação;
- testes;
- saídas.

O que chamamos de hardware sã os equipamentos mainframe: PCs, notebooks, servidores dedicados, tablets, smartphones, roteadores, switches, impressoras, coletores de dados, leitores de código de barras e QR Code, entre outros.

Os softwares são os sistemas operacionais, aplicativos (programas), protocolos de comunicação, antivírus, soluções de ERP, certificados digitais, tecnologias como blockchain, entre muitos outros.

2.4 Aspectos da tríade CID

Para que um sistema de informações ofereça estabilidade e segurança, os usuários das informações armazenadas devem contar com a tríade CID, que se refere a confidencialidade, integridade e disponibilidade.

A confidencialidade é um aspecto que garante que todas as informações possam ser acessadas somente por pessoas autorizadas. Este aspecto exige mecanismos de segurança como nomes de usuário, senhas, listas de controle de acesso, também conhecida como ACLs (access control list), tokens e criptografia.

As informações são categorizadas de acordo com o seu nível de criticidade, isto é, são definidos padrões que analisam qual o dano que um acesso indevido poderia causar caso ocorresse e suas consequências.

A confidencialidade também está relacionada ao princípio do "menor privilégio", que estabelece acesso apenas a poucas pessoas, conforme a necessidade de conhecimento e o seu nível de responsabilidade.

Está modalidade da tríade possui algumas características:

- identificação;
- autenticação;
- autorização;
- controle de acesso;
- privacidade.

Sendo assim, as informações confidenciais também podem ser compartilhadas ou armazenadas em outras mídias, porém, neste caso a criptografia é uma forma de preservar a confidencialidade até a sua total eliminação (descarte) pelo sistema.

O princípio de integridade é o que garante que as informações, tanto em sistemas periféricos quanto em bancos de dados, estejam armazenadas corretamente desde a sua inclusão ou possíveis alterações. O que significa dizer que a informação uma vez gravada permanecerá intacta até que seja alterada ou eliminada por uma pessoa autorizada.

O princípio da disponibilidade garante que as informações e os recursos estejam disponíveis para os usuários que precisam deles de modo permanente, ou seja, 24 horas por dia, sete dias por semana. Esta função atualmente também pode ser disponibilizada através da tecnologia cloud computing (computação em nuvem), cujas informações podem ser acessadas pelos usuários autorizados em qualquer localidade do planeta e que disponham de acesso à rede mundial de computadores (Internet).

2.5 Definição de ameaça, risco e vulnerabilidade

Antes de abordarmos os conceitos de ameaças, riscos e vulnerabilidades, é importante frisar sobre o que essas três situações poderiam causar na organização, e o mais importante: o que elas poderiam comprometer.

Estamos assim falando sobre os ativos da organização, que são as pessoas, propriedades e informações. Podemos incluir como pessoas os funcionários e clientes ou contratados. As propriedades são os ativos imobiliários, e consistem em itens tangíveis e intangíveis que possuem um determinado valor. Os ativos intangíveis se referem a reputação e informações proprietárias. As informações pertencem aos bancos de dados, o código-fonte dos softwares, registros críticos da

empresa, fórmulas, procedimentos e muitos outros itens intangíveis. Agora vamos compreender os seguintes conceitos:

- Ameaça: é qualquer coisa que possa explorar uma vulnerabilidade, intencional ou acidental, e copiar, modificar, danificar ou destruir um ativo. Elas podem ser identificadas, mas via de regra fogem ao nosso controle.

- Risco: podem ser internos ou externos. Qualquer evento que possa causar impacto na capacidade das organizações atingirem seus objetivos de negócio. Em suma, é uma possibilidade de corromper um ativo através de ameaças e vulnerabilidades.

- Vulnerabilidade: é uma fraqueza ou um grande rombo em um programa de segurança que pode ser explorado para obter acesso não autorizado a um ativo. É uma falha no sistema de proteção que pode trazer prejuízos incalculáveis à organização.

É muito importante compreender a diferença entre ameaças, vulnerabilidades e riscos. Com isso podemos concluir que:

Ativo + Ameaça + Vulnerabilidade = Risco

2.6 Diferença entre acidente, incidente e desastre

Podemos definir esses elementos como:

- Acidente: acontecimento casual, fortuito, inesperado; ocorrência; qualquer acontecimento, desagradável ou infeliz, que envolva dano, perda, sofrimento ou morte.

- Incidente: quer dizer que incide, sobrevém; que possui caráter acessório, secundário; superveniente.

A diferença entre esses dois substantivos pode ser estabelecida tendo como parâmetro as consequências de cada ocorrência.

Enquanto o acidente causa algum tipo de lesão, o incidente não apresenta nenhum dano.

- Desastre: pode ser considerado como qualquer circunstância, evento, acontecimento que pode provocar um prejuízo imenso, de grandes consequências.

Trazendo estas ocorrências para a tecnologia da informação e também para a os sistemas de segurança, poderemos considerar que:

- Acidente é uma ocorrência inesperada que pode parar toda uma fábrica em função dos computadores estarem desligados por uma sobrecarga elétrica, ou talvez uma inundação nos servidores que paralisem todos os sistemas de produção.
- Incidente é uma ocorrência de pequeno porte, mas que pode causar danos na utilização dos sistemas e com isso atrasar pedidos, processos em andamento, entre outros.
- Desastre já pode ser considerado como uma ocorrência de dimensões muito maiores. Um incêndio, uma inundação, uma invasão feita por um hacker ou um programa malicioso que pode adulterar todo o sistema e causar danos irrecuperáveis.

2.7 Política de segurança: conceito, tipos e criação

De acordo com a norma ISO 27001, a Política de Segurança da Informação, também conhecida como PSI, é definida como uma norma que reúne um conjunto de ações, técnicas e boas práticas para o uso seguro de dados empresariais; isto é, um manual que estabelece quais medidas são as mais importantes para atestar a segurança de dados da organização.

A PSI não é uma norma opcional. Ela é obrigatória e determina o funcionamento de como os ativos de TI devem ser protegidos, como os

profissionais da área devem agir no caso de ameaças e quais atitudes tomar para evitar ou recuperar os ativos no caso de alguma violação.

Existem vários tipos de PSI, dos quais podemos destacar os mais importantes:

- Definir cronogramas de backup (cópias de segurança).
- Estabelecer regras para o uso de senhas e credenciais de acesso.
- Controlar o acesso aos espaços físicos.
- Definir as políticas de atualização e versionamento de softwares.
- Definir diretrizes para o acesso à informação de diferentes profissionais e equipes, estabelecendo graus de acessibilidade.
- Criar planos de contingência e de gerenciamento de riscos.

A implantação de uma Política de Segurança da Informação exige a participação de todos os colaboradores da organização, no entanto, é de fundamental importância a consciência e a participação colaborativa de todos sem exceção para que a PSI tenha sucesso.

2.8 Gerenciamento de ativos

De acordo com a Norma Técnica ISO 55000, ativo é todo e qualquer bem sobre o qual a organização possui controle. Os ativos podem ser classificados como tangíveis, como os bens materiais, ou intangíveis, como todo o conhecimento intelectual da organização.

Sendo assim, podemos entender que os ativos são os bens materiais e imateriais que compõem o patrimônio de uma organização. Alguns exemplos de ativos são:

- ferramentas de trabalho

- equipamentos de TI
- softwares
- máquinas industriais
- materiais de escritório
- veículos de uma frota
- produto acabado e matéria-prima
- contratos em andamento
- patrimônio intelectual
- experiência
- know-how

A gestão de ativos é o conjunto de atividades voltadas para obter valor dos ativos da empresa, como balanceamento de custos, oportunidades e riscos, performance esperada dos ativos etc.

Antes de ser adquirido, o ativo deve ser estudado minuciosamente para que, ao entrar definitivamente como um ativo, ele possa ser explorado em toda sua plenitude e ser mantido adequadamente por toda sua vida útil.

2.9 Conformidade (compliance)

A palavra 'compliance' é um termo da língua inglesa que significa 'conformidade', e está diretamente relacionada ao cumprimento de leis e de normas internas e externas pela organização. É um sistema de políticas, procedimentos e diretrizes éticas que uma organização adota e que visa normatizar e assegurar a atuação de seus colaboradores e fornecedores.

O compliance ganhou muita notoriedade a partir da Lei Anticorrupção (Lei nº 12.846/2013). O crescimento dessa prática entre as empresas no Brasil já ganhou muitas adesões e estima-se que 64% das organizações possuem um processo de avaliação e riscos de compliance, mas ainda não há informações consolidadas a respeito da adesão no Brasil.

Em muitos casos, o maior enfoque no compliance está na gestão, isto é, no desenvolvimento organizacional de uma cultura ética e transparente. O compliance pode trazer muitos benefícios para a organização como, por exemplo: os ganhos de oportunidade de negócios e vantagem competitiva; a melhora da imagem da empresa no mercado; desperta a atração de investimentos; reduz o número de fraudes e corrupção; melhora os resultados financeiros; e traz para os colaboradores maior satisfação e produtividade.

Considerações finais

Neste capítulo apresentamos a norma ISO 27000 e todas as suas normas complementares. Com isso, desenvolvemos muitos assuntos que são fundamentais para a segurança de uma área de TI, tais como definição sobre informação e dado, as formas da informação e sistemas de TI. Passamos a conhecer a tríade CID, o que são ameaças, incidentes e desastres, bem como o que é uma política de segurança, gerenciamento de ativos e compliance.

Por mais que haja esforço de nossa parte em detalhar as informações apresentadas neste capítulo, a pesquisa e o aprendizado complementar são compromissos que não se deve desprezar, portanto, busque sempre estender seu conhecimento através da pesquisa e explorar o assunto em toda sua plenitude.

Referências

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. **Diário Oficial**: seção 1, p. 1, Brasília, DF, 2 ago. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 15 maio 2021.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. São Paulo: Atlas, 2012.

STEWART, Thomas A. **Capital intelectual**: a nova vantagem competitiva das empresas. Rio de Janeiro: Campus, 1998.