1.Introdução

A política de segurança da informação é uma coisa, implementá-la na organização e checar se ela está sendo cumprida é outra. Muitas organizações trabalham com ciclo PDCA (Plan, Do, Check, Act). A política de segurança da informação é o principal documento. A política de segurança da informação inclui documentos de política, procedimentos e orientações que visam um determinado aspecto de segurança da informação e que fornecem expectativas detalhadas. Esses documentos são uma parte importante do Sistema de Gestão da Segurança da Informação (ISMS).

2.Implantação de ISMS

A organização formula uma estrutura para o controle do seu ISMS. Essa estrutura fornece uma classificação lógica de todas as questões relacionadas à segurança da informação, organizando-as em domínios.

Um domínio é um grupo de assuntos que estão logicamente conectados uns aos outros. Os domínios formam a base para a estrutura ISMS. Esses domínios algumas vezes possuem seus próprios documentos de política, procedimentos e instruções de trabalho. Os requisitos estabelecidos na norma ISO 27001:2013 são genéricos e aplicáveis a todas as organizações, independentemente de tipo, tamanho ou natureza.

3.Entendendo a organização e seu contexto

A organização precisa definir as questões externas e internas que são relevantes para o seu propósito e que afetam sua habilidade de alcançar o(s) resultados(s) pretendido(s) do seu sistema de gerência de segurança da informação.

4.Compreendendo as necessidades e expectativas das partes interessadas

Enquanto a ISO 27001:2005 focava internamente, as organizações colaboradoras da ISO percebem que no período entre 2005 e 2013 o mundo havia mudado. Organizações estão mais e mais conectadas. Muitas vezes os sistemas de informação são terceirizados, a informação é compartilhada com outras empresas com quem têm relação ou organismos governamentais. Os requisitos das partes interessadas podem incluir requisitos legais e regulatórios e obrigações contratuais. A organização deve, portanto, definir: as partes interessadas que são relevantes para o sistema de gerenciamento de segurança da informação; os requisitos relevantes dessas partes interessadas para a segurança da informação.

5.Definindo o escopo do Sistema de Gerenciamento de Segurança da Informação (SGSI)

A organização deve definir os limites e a aplicabilidade do sistema de gerenciamento de segurança da informação, a fim de estabelecer seu escopo. Ao definir o seu escopo, a organização deve considerar as questões internas e externas, conforme previamente descrito, as interfaces e dependências entre as atividades desempenhadas pela organização, bem como aquelas desempenhadas por outras organizações e que são aplicáveis ao escopo da organização. O escopo deve estar disponível como informação documentada.

6.O modelo PDCA

O modelo PDCA (Plan-Do-Check-Act), também chamado de ciclo de qualidade de Deming, forma a base para determinar, implementar, monitorar, controlar e manter o sistema de gerenciamento da segurança da informação (ISMS).

A ISO 27001:2005 exige o modelo PDCA como a base geral para a implementação e a manutenção do ciclo de gestão.

Na ISO 27001:2013 isso mudou. A ISO percebeu que a maioria das empresas e organizações com ou sem fins lucrativos já possui seu próprio ciclo de gestão de negócios, sendo ou não baseado no PDCA. PDCA nem sempre é compatível com o ciclo de gestão adotado por uma empresa em particular. Por essa razão, na ISO 27001:2013 o texto mudou para a obrigação da organização estabelecer, implementar, manter e melhorar continuamente o sistema de gerenciamento da segurança da informação, em conformidade com os requisitos dessa norma internacional. É claro que a norma apresenta requisitos para estabelecer o ISMS. No entanto, a obrigação de utilizar o ciclo PDCA desapareceu.

6.1 Projetar o ISMS (Planejar)

Na fase de projeto, é desenvolvida e documentada a política de segurança da informação. Aqui os objetivos da segurança da informação, os processos relevantes e os procedimentos são definidos; isso assegura que os riscos sejam gerenciados. Esses objetivos devem, é claro, apoiar os objetivos de negócios da organização. As medidas de segurança podem ser adotadas com base em uma análise de riscos e de custo-benefício. A fase de planejamento se aplica não só à política principal, mas também a todos os documentos de políticas que apoiam e as regulamentações subjacentes.

6.2 Implementar o ISMS (Executar)

Nesta fase, a política de segurança da informação e os procedimentos e medidas subjacentes são implementados. As responsabilidades são alocadas a cada sistema e/ou processo de informação.

6.3 Monitorar e checar o ISMS (Checar)

Nesta fase, são realizados controles utilizando uma autoavaliação e, onde possível, medições são realizadas para ver se a política de segurança da informação é executada corretamente. Um relatório sobre o assunto é emitido para gerência responsável e para o Diretor Corporativo de Segurança da Informação (CISO).

6.4 Manter e ajustar o ISMS (Agir)

Nesta fase final, são realizadas correções e são tomadas medidas preventivas com base nos resultados da auditoria interna. O ISMS é atualizado à luz de quaisquer descobertas particulares. O ciclo PDCA é contínuo. Isso está descrito em um manual ISMS.

7.Posse ou controle

Suponha que um ladrão roube um envelope lacrado contendo um cartão bancário de débito e a senha associada ao cartão. Mesmo que o ladrão não abra esse envelope, a vítima do roubo ficaria legitimamente preocupada com a possibilidade do ladrão usar o cartão de forma fraudulenta e a qualquer momento sem o controle do proprietário. Essa situação ilustra uma perda de controle ou posse de informações, mas não envolve a quebra de sigilo.

8.Autenticidade

Autenticidade se refere à veracidade da alegação de origem ou a auditoria das informações. Por exemplo, um método de verificação da auditoria de um documento escrito à mão é comparar as características de escrita do documento com uma amostra de outros que já tenham sido verificados. Para informações eletrônicas, uma assinatura digital pode ser usada para verificar a autoria de um documento digital usando criptografia de chave pública.

9.Utilidade

Utilidade significa capacidade de uso. Suponha que alguém criptografar dados em um disco para prevenir o acesso não autorizado ou modificações indesejadas - e depois perdeu a chave criptográfica: isso seria uma quebra de utilidade. Os dados seriam confidenciais, controlados, integrais, autênticos e disponíveis - eles não seriam úteis dessa forma. Similarmente, a conversão de dados salariais de uma moeda para outra inadequada também seria uma quebra de utilidade, assim como seria o armazenamento de dados em um formato impróprio para uma determinada arquitetura de computador. A substituição de uma tabela de dados por um gráfico poderia ser descrita como uma quebra de utilidade se a substituição tornar mais difícil a interpretação dos dados. A utilidade é muitas vezes confundida com disponibilidade, pois as falhas, também podem requerer tempo para solucionar as alterações de formato ou de apresentação dos dados. Entretanto, o conceito de capacidade de uso é diferente do de disponibilidade.

10.Devida diligência e devido cuidado

Hoje, as devidas diligências e devidos cuidados estão se tornando questões sérias nas operações de computadores. De fato, o sistema legal começou a responsabilizar importantes parceiros pela ausência dos devidos cuidados no caso de uma grave falha de segurança. Violações de segurança e privacidade são questões quentes que confrontam a comunidade da Internet, e são necessárias normas que abranjam as melhores práticas de devidos cuidados para a proteção de uma organização.

Requisito de Segurança	Risco de Negócio
Privacidade e Criptografia no Nível de Transporte	Confidencialidade e Integridade
Controle de Autenticação	Confidencialidade, Integridade e Disponibilidade
Controle de Autorização	Confidencialidade, Integridade e

	Disponibilidade

Devida diligência consiste em compreender as ameaças e os riscos atuais, e devido cuidado diz respeito à implementação de contramedidas para prover proteção contra essas ameaças. Se uma empresa não pratica o devido cuidado e a devida diligência em relação à segurança de seus ativos, ela pode ser legalmente acusada de negligência e responsabilidade por quaisquer implicações dessa negligência de acordo com as leis de cada país em que opera, se for um negócio.

11.Devida diligência e devido cuidado

11.1 Diferença entre dado e informação

É essencial compreender a diferença entre dado e informação. O dado pode ser processado pela tecnologia da informação, mas ele se torna informação após adquirir certo significado. Quando se trata de segurança da informação, você deve levar em conta as diversas formas nas quais a informação pode essencialmente se concentrar. Isso envolve, afinal de contas, a segurança da própria informação e independe da forma em que ela é apresentada. No entanto, isso impõe algumas restrições acerca das medidas necessárias para proteger essa informação.

11.2 Análise da informação

A análise da informação fornece uma imagem clara de como uma organização lida com a informação. Por exemplo, um hóspede se registra em um hotel através do site. Essa informação é passada para o sistema de reservas on-line, que, em serviços domésticos, sabe que o quarto deve estar limpo para a chegada do hóspede. Em todos esses passos, é importante que a informação seja confiável.

11.2.1 Informática

Informática é converter dados em informação. A informática desenvolve novos usos para a tecnologia da informação, está interessada em como as pessoas transformam a tecnologia e em como a tecnologia nos transforma.

11.3 O valor do dado

O dado pode ter grande importância, mesmo se ele não estiver no formato de “informação”, como definido anteriormente. Não haveria a necessidade da “proteção dos dados” e, portanto, da “segurança de computadores” se dados, por definição, não tivessem importância. O valor do dado é determinado principalmente pelo usuário.

11.4 O valor da informação

Informação é conhecimento que alguém tenha adquirido. Enquanto algumas pessoas podem considerar um determinado conjunto de dados desinteressante, outros podem ser capazes de extrair informações valiosas a partir dele. O valor da informação é, portanto, determinado pelo valor que o beneficiário lhe atribui.

11.5 Informação como um fator de produção

Os fatores de produção normais de uma empresa ou organização são o capital, o trabalho (manual) e as matérias-primas. Em tecnologia da informação, é comum também considerar a informação como fator de produção. Empresas não podem existir sem informação. Um armazém que perde suas informações de estoque e clientes normalmente não seria capaz de operar sem elas. Para algumas empresas, tais como o escritório de um contador, a informação é, na verdade, o seu único produto.

11.6 Sistemas de Informação

A transferência e o processamento de informações ocorrem através de uma infraestrutura de sistema de informação. O termo sistema de informação é frequentemente usado para se referir à interação entre pessoas, processos, dados e tecnologia. Nesse sentido, o termo é usado para se referir não só à tecnologia da informação e da comunicação (TIC) que uma organização usa, mas também à forma como as pessoas interagem com essa tecnologia em apoio aos processos de negócio. Exemplos de sistemas de informação são documentos em armários de arquivos, arquivos de computador e bases de dados, telefones celulares e impressoras. No contexto da segurança da informação, um sistema de informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional.

Componentes de TIC incluem:

1. Estações de trabalho, que consistem em um PC com um sistema operacional e outros softwares.
2. Transporte de dados através de uma rede, cabeada ou sem fio
3. Servidores, que consistem no servidor com um sistema operacional e softwares
4. Armazenamento de dados, como em disco, e-mail e bancos de dados
5. Telefones móveis que evoluem cada vez mais para pequenos dispositivos computacionais com grande armazenamento removível.
6. A capacidade e a possibilidade de trocar informações pela rede móvel e/ou bluetooth.
7. Conexões

Um armário de arquivos é uma peça do mobiliário de escritório normalmente usado para armazenar documentos de papel em pastas.

12.Gestão da Informação

A gestão da informação descreve o meio pelo qual uma organização planeja, coleta, organiza, utiliza, controla, dissemina e descarta suas informações de forma eficiente, e através da qual garante que o valor dessa informação seja identificado e explorado em toda sua extensão. Quando você traduz essa definição para o portugu~es, pode dizer que este campo interdisciplinar se baseia em e combina habilidades e recursos de:

1. Biblioteconomia e ciência da informação
2. Tecnologia da informação
3. Arquivamento e administração geral

Livros e periódicos, dados armazenados em computadores locais ou remotos, microformas, mídias audiovisuais e informações na cabeça das pessoas estão em todos dentro desse escopo. Alguns dos principais tópicos com que os profissionais se preocupam são:
1. Classificação e codificação
2. Indexação de assunto
3. Construção e uso de dicionários e vocabulários controlados
4. Catalogação e indexação por nomes, lugares e eventos
5. Projeto de banco de dados e estruturas de dados
6. Armazenamento físico de livros e registros, em papel e em formato eletrônico
7. Armazenamento de imagens fotográficas e digitalizadas
8. Auditorias de informação: revisão dos recursos de informação de uma organização
9. Documentação de objetos de museu, tanto para fins de administração quanto como um recurso para estudos

13.Computação distribuída

A tendência da computação distribuída também enfraqueceu a eficácia do controle central e especializado. Em geral, a computação distribuída é qualquer computação que envolve vários computadores distantes um do outro, onde cada um tem um papel no problema computacional ou no processamento da informação. Em empresas comerciais, computação distribuída geralmente significa colocar vários passos dos processos de negócios nos locais mais eficientes, em uma rede de computadores. Em uma transação típica, o processamento da interface do usuário é feito em um PC situado no local do usuário, o processamento do negócio é feito em um computador remoto e o processamento e o acesso à base de dados são realizados em outro computador que fornece acesso centralizado para muitos processos do negócio. Tipicamente, esse tipo de computação distribuída usa o modelo de comunicação cliente/servidor.

O Ambiente de Computação Distribuída (DCE), é um padrão industrial amplamente utilizado que suporta esse tipo de comunicação distribuída. Na Internet, provedores de serviço terceirizados já oferecem alguns serviços generalizados que se encaixam nesse modelo. Um serviço de diretório possui um banco de dados hierárquico de usuários, computadores, impressoras, recursos e atributos de cada um destes. O diretório é usado principalmente para operações de consulta, o que habilita os usuários a rastrear recursos e outros usuários. O administrador pode então desenvolver políticas de controle de acesso, segurança e auditoria que ditem quem pode acessar esses objetos, como eles são acessados e auditar cada uma dessas ações. Mais recentemente, a computação distribuída é usada para se referir a toda grande colaboração na qual muitos proprietários de computadores pessoais permitem que parte do tempo de processamento de seus computadores seja posto a serviço de um grande problema.

14.Processos operacionais e informações

O gerenciamento abrange uma vasta gama de atividades elaboradas para melhorar a eficácia e a eficiência de uma organização. Para entender toda a gama de ações de gestão, e para desenvolver o conhecimento e a habilidade para desempenhar essas atividades, podemos classificar o conjunto completo de atividades de gestão de diferentes maneiras. Uma forma de classificar as atividades de gestão se baseia nas dimensões da totalidade do desempenho organizacional no qual está sendo focado. Para gerenciar uma organização de forma eficaz, os gestores precisam focar em toda a organização como uma só unidade, mas ao mesmo tempo, precisam prestar atenção individual a cada pequena atividade realizada.

Ao classificar a gestão em termos da totalidade do desempenho organizacional, podemos definir uma série contínua de níveis de gestão que vão desde a gestão estratégica, em uma extremidade, até a gestão operacional, na outra. Gestão estratégica se concentra no desempenho da organização completa. O foco aqui é determinar os objetivos mais adequados que a organização deve buscar, dadas suas forças e fraquezas internas, bem como as oportunidades e ameaças externas enfrentadas por ela.

A gestão estratégica implica em alcançar um equilíbrio entre os requisitos das diferentes funções e unidades da organização. Ela também implica em equilibrar os riscos, tanto em curto como em longo prazo. Uma característica única da gestão estratégica é a ausência de quaisquer planos ou objetivos de nível mais elevado para orientar a ação de gestão estratégica.

A gestão operacional está na outra extremidade da série contínua de níveis de gestão. Ela diz respeito à garantia de que as operações do dia-a-dia da organização sejam levadas a cabo com eficácia e eficiência.

O nível entre a gestão estratégica e a gestão operacional é a gestão tática. Esse nível de gestão está preocupado com o planejamento e controle para funções organizacionais individuais tais como marketing, produção e desenvolvimento de recursos humanos, ou funções abaixo destas, destinadas a melhorar o desempenho a curto e médio prazo. No nível de processos de negócios, as coisas acontecem em geral da mesma forma como previamente descrito. Cada método de negócio é um conjunto de atividades ou tarefas relacionadas e estruturadas que desenvolvem um produto ou serviço específico para um cliente ou clientes específicos.

Um processo de negócio começa com a necessidade de um cliente e termina com a satisfação dessas necessidades. Organizações orientadas a processos quebram as barreiras dos departamentos estruturais e tentam evitar silos funcionais. Um processo de negócio pode ser decomposto em diversos subprocessos, os quais têm seus próprios atributos, mas que também contribuem para o atingimento da meta do superprocesso. A análise dos processos de negócio tipicamente inclui o mapeamento de processos e subprocessos até o nível de atividade. Processos de negócios são projetados para adicionar valor ao cliente e não devem incluir

atividades desnecessárias. O resultado de um processo de negócio bem projetado é o aumento da eficácia e o aumento da eficiência.

15.Arquitetura da informação

Segurança da informação está intimamente relacionada à arquitetura da informação. Ao projetar sistemas de informação, é necessário pensar na segurança da informação desde o início.

A arquitetura de estrutura corporativa mais usada é a TOGAF (The Open Group Architecture Framework). A arquitetura da informação é uma parte importante da arquitetura corporativa. A TOGAF permite projetar, avaliar e desenvolver a arquitetura certa para a sua organização. A chave para a TOGAF é o ADM (Architecture Development Method), que é um método confiável e comprovado para desenvolver uma arquitetura corporativa de TI que atenda às necessidades do seu negócio.

A maioria das definições têm qualidades em comum: um projeto estrutural de ambientes compartilhados, métodos de organizar e de rotular websites, intranets e comunidades on-line, e maneiras de trazer os princípios de design e arquitetura para o cenário digital. Organizar a funcionalidade e o conteúdo em uma estrutura na qual as pessoas sejam capazes de navegar intuitivamente não acontece por acaso. As organizações devem reconhecer a importância da arquitetura da informação ou então elas correm o risco de criar grandes conteúdos e funcionalidades que ninguém nunca vai encontrar. Também se discute a relação entre a arquitetura da informação e a usabilidade no contexto de projetos reais.

A enorme fartura de funcionalidades e informações tornou-se o novo problema. O desafio enfrentado pelas organizações é: como orientar as pessoas através da vasta quantidade de informações ofertadas, de forma que elas possam encontrar com sucesso a informação que desejam e, assim, encontrar valor no sistema. Uma arquitetura da informação eficaz permite que as pessoas adentrem logicamente no sistema confiantes de que estão se aproximando da informação de que necessitam. A maioria das pessoas só percebe a arquitetura da informação quando esta é pobre e os impede de encontrar as informações de que necessitam.