1.Definições e Conceitos de Segurança da Informação

1.1 Ação preventiva

Ação para eliminar a causa de uma potencial não conformidade ou outra potencial situação indesejável

1.2 Aceitação do risco

A decisão de aceitar um risco

1.3 Ameaça

Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização

1.4 Análise da Informação

A análise da informação proporciona uma clara imagem de como uma organização manuseia a informação

1.5 Análise de riscos

Um processo para compreender a natureza do risco a fim de determinar o seu nível. Uma análise de riscos proporciona a base para a estimativa do risco e para as decisões sobre o tratamento do risco. A análise de riscos inclui a estimativa do risco

1.6 Ataque

Uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de, um ativo

1.7 Ativo

Qualquer coisa que tenha valor para a organização. Eta é uma definição ampla, você pode pensar em instalações, informações, software, hardware, serviços impressos, mas também em pessoas, habilidades, experiências e coisas intangíveis, como reputação e também imagem

1.8 Autenticidade

Propriedade de uma entidade ser o que afirma que é

1.9 Avaliação do risco

A avaliação do risco é o processo geral de identificação do risco, análise do risco e estimativa do risco

1.10 Confiabilidade

Propriedade de consistência dos comportamentos e resultados desejados

1.11 Confidencialidade

Propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados. O conceito de confidencialidade busca prevenir a divulgação intencional ou não intencional do conteúdo de uma mensagem. A perda de confidencialidade pode ocorrer de diversas maneiras tais como pela divulgação intencional de uma informação privada de uma empresa ou pelo mau uso das credenciais de acesso à rede

1.12 Controle

Meios de gerenciar o risco, incluindo políticas, procedimentos, diretrizes e práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modifiquem o risco à segurança da informação. É possível que os controles nem sempre exerçam os pretendidos ou assumidos efeitos de mudança, e o controle também é usado como sinônimo para salvaguarda ou contramedida

1.13 Diretriz

Descrição que esclarece o que deve ser feito, e como, para alcançar os objetivos definidos nas políticas

1.14 Disponibilidade

Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. O texto formal anterior assegurava o acesso confiável e em tempo oportuno a dados ou recursos de computação pelo pessoal apropriado. A disponibilidade garante que os sistemas estão ativos e funcionando quando necessário

1.15 Estimativa de risco

É o processo de comprar os resultados de análise do risco com um critério de risco a fim de determinar quando o risco e/ou sua magnitude é aceitável ou tolerável

1.16 Evento de segurança da informação

Ocorrência identificada de um estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou falha de proteção, ou uma situação previamente desconhecida que possa ser relevante em termos de segurança

1.17 Exposição

Exposição é a circunstância de estar exposto aos prejuízos oriundos de um agente ameaçador

1.18 Gerenciamento de riscos

Atividades coordenadas para direcionar e controlar uma organização no que diz respeito ao risco

1.19 Gestão da informação

A gestão da informação descreve os meios pelos quais uma organização eficientemente planeja, coleta, organiza, usa, controla, dissemina e descarta sua informação, e através da qual garante que o valor dessa informação é identificado e explorado em toda a sua extensão

1.20 Gestão de incidentes de segurança da informação

Processos para detectar, reportar, avaliar, responder, lidar e aprender com os incidentes de segurança da informação

1.21 Gestão de segurança da informação

Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. O gerenciamento do risco tipicamente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco

1.22 Identificação do risco

É o processo de encontrar, reconhecer e descrever riscos. A identificação do risco envolve a identificação das suas fontes, eventos, causas e suas potenciais consequências. A identificação do risco também pode envolver dados históricos, análise teórica, opiniões, pareceres fundamentados e de especialistas, e necessidade das partes interessadas

1.22 Incidente de segurança da informação

Um incidente de segurança da informação é indicado por um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação

1.23 Informação

Informação é o dado que tem significado em algum contexto para quem o recebe. Quando a informação é inserida e armazenada em um computador, ela é geralmente referida como dado. Após processamento, o dado de saída pode ser novamente percebido como informação

1.24 Instalação de processamento de informações

Qualquer sistema de processamento de informações, serviço ou infraestrutura, ou os locais físicos que as abriguem

1.25 Integridade

Propriedade de proteger a exatidão e a integridade dos ativos. O conceito de integridade assegura que sejam prevenidas modificações não autorizadas ao software e ao hardware, que não sejam feitas modificações não autorizadas aos dados, por pessoal

autorizado ou não autorizado e/ou processo, e que o dado seja internamente e externamente consistente

1.26 Não repúdio

Habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades de origem

1.27 Política

A intenção e orientação geral formalmente expressa pela administração

1.28 Procedimento

Forma específica de conduzir uma atividade ou processo

1.29 Processo

Conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas

1.30 Processo de gerenciamento de riscos

É a aplicação sistemática de políticas de gerenciamento, procedimentos e práticas às atividades de comunicar, consultar, estabelecer o contexto e identificar, analisar, avaliar, tratar, monitorar e revisar o risco. A ISO/IEC 27005:201, norma para o gerenciamento do risco à segurança da informação, usa o termo “processo” para descrever todo o gerenciamento de riscos. Os elementos dentro do processo de gerenciamento de riscos são denominados “atividades”

1.31 Responsabilidade

Atribuição de ações e decisões a uma entidade

1.32 Riscos

Efeito da incerteza sobre os objetivos. É a combinação da probabilidade de um evento e sua consequência. Um efeito é um desvio do que é esperado, o qual pode ser positivo e/ou negativo. Os objetivos podem ter diferentes aspectos (tais como financeiro, saúde e segurança, segurança da informação e metas ambientais) e podem ser aplicados em diferentes níveis (tais como estratégico, em toda a organização, projeto, produto e processo). Um risco é frequentemente caracterizado pela referência a potenciais eventos e consequências, ou uma combinação destes. O risco à segurança da informação é muitas vezes expresso em termos de uma combinação entre as consequências de um evento de segurança da informação e sua probabilidade de ocorrência. Incerteza é o estado, mesmo que parcial, de deficiência da informação relacionada a compreensão ou conhecimento de um evento, sua consequência ou probabilidade. O risco à segurança da informação está associado ao potencial de

ameaças explorarem vulnerabilidades de um ativo de informação ou grupo de ativo de informações e, desse modo, causar danos a uma organização

1.33 Risco residual

Risco que permanece após o tratamento do risco. O risco residual pode conter riscos não identificados e também pode ser conhecido como “risco retido”

1.34 Segurança da informação

Preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem ser incluídas. Podemos dizer que a segurança da informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio

1.35 Sistema de Gerenciamento da Segurança da Informação (SGSI)

Parte do sistema total de gerenciamento, baseado em uma abordagem de riscos de negócios, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. O sistema de gerenciamento inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos

1.36 Sistema de informação

Aplicação, serviço, recursos de tecnologia da informação ou qualquer outro componente de manejo da informação. Em um sentido bem amplo, o termo sistema da 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 somente à Tecnologia da Informação e de Comunicação (TIC) que uma organização usa, mas também à forma como as pessoas interagem com essa tecnologia em apoio aos processos de negócio

1.37 Terceiro

A pessoa é reconhecida como sendo independente das outras partes envolvidas, até onde diz respeito ao assunto em questão

1.38 Tratamento de risco

É o processo de seleção e implementação de medidas para modificar os riscos. O tratamento de riscos pode envolver: evitar o risco ao optar por não começar ou continuar com a atividade que dá origem ao risco; tomar ou elevar o risco a fim de perseguir uma oportunidade; remover a fonte de risco; alterar a probabilidade; alterar as consequências; dividir o risco com um terceiro ou terceiros; manter o risco através de uma escolha consciente

1.39 Vulnerabilidade

Fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças

2.Conceitos de segurança

Antes de definir uma estratégia de segurança, é preciso saber o que estamos protegendo e do que estamos protegendo. A metodologia que empregamos para nos ajudar a obter algum conhecimento sobre isso é chamada de análise do risco. Existem várias formas de realizar uma análise do risco.

Requisitos de segurança **são identificados através de uma avaliação metódica de riscos de segurança**. As despesas com controles devem ser equilibradas de acordo com os danos resultantes de falhas de segurança, mais prováveis de ocorrer no negócio.

Os resultados da avaliação do risco ajudarão a guiar e a determinar a ação apropriada de gestão e as propriedades para gerenciar os riscos de segurança da informação e para implementar os controles escolhidos para proteção contra riscos e ameaças.

A avaliação do risco deve ser repetida periodicamente para tratar qualquer mudança que possa influenciar os resultados da avaliação do risco.

A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados onde necessário, para assegurar que os objetivos de segurança e do negócio da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gerenciamento de negócio.

A abordagem de processo para a gestão de segurança da informação apresentada na ISO 27001:2013 inclui:

01. Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação.

02. Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócios da organização.

03. Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (ISMS)

04. Melhoria contínua baseada em medições objetivas

A informação e os processos de apoio, os sistemas e as redes são ativos de negócios importantes. Definir, alcançar, manter e melhorar a segurança da informação pode ser essencial para manter a vantagem competitiva, o fluxo de caixa, a rentabilidade, a observância da lei e a imagem comercial.

As organizações e seus sistemas de informação e redes enfrentam ameaças de segurança provenientes de um amplo leque de fontes, incluindo fraudes assistidas por computador, espionagem, sabotagem, vandalismo, incêndio ou inundação. As causas de danos, como códigos maliciosos, atividades de hacking em computadores e ataques de negação de serviço se tornam mais comuns, mais ambiciosos e cada vez mais sofisticados.

A segurança da informação é importante tanto para os negócios públicos quanto para o setor privado, e para proteger infraestruturas críticas. Em ambos os setores a segurança da informação funcionará como uma facilitadora para evitar ou reduzir os riscos relevantes.

A interconexão de redes públicas e privadas e o compartilhamento dos recursos de informação aumentam a dificuldade de se seguir controle de acesso.