1.Definições e Conceitos de Segurança da Informação

Conceitos	Descrição
Ação preventiva	Ação para eliminar a causa de uma potencial não conformidade ou outra potencial situação indesejável
Aceitação do risco	A decisão de aceitar um risco
Ameaça	Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização
Análise da informação	A análise da informação proporciona uma clara imagem de como uma organização manuseia a informação
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
Ataque	Uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de, um ativo
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
Autenticidade	Propriedade de uma entidade ser o que afirma que é
Avaliação do risco	A avaliação do risco é o processo geral de identificação do risco, análise do risco e estimativa do risco
Confiabilidade	Propriedade de consistência dos comportamentos e resultados desejados
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

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
Diretriz	Descrição que esclarece o que deve ser feito, e como, para alcançar os objetivos definidos nas políticas
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
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
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
Exposição	Exposição é a circunstância de estar exposto aos prejuízos oriundos de um agente ameaçador
Gerenciamento de riscos	Atividades coordenadas para direcionar e controlar uma organização no que diz respeito ao risco
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
Gestão de incidentes de segurança da informação	Processos para detectar, reportar, avaliar, responder, lidar e aprender com os incidentes de segurança da informação
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
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
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
Informação	Informação é o dado que tem significado em algum contexto para quem o receve. 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
Instalação de processamento de informações	Qualquer sistema de processamento de informações, serviço ou infraestrutura, ou os locais físicos que as abriguem
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
Não repúdio	Habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades de origem
Política	A intenção e orientação geral formalmente expressa pela administração
Procedimento	Forma específica de conduzir uma atividade ou processo
Processo	Conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas

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"
Responsabilidade	Atribuição de ações e decisões a uma entidade
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
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"
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

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

- **1.** Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação.
- **2.** Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócios da organização.
- **3.** Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (ISMS)
- **4.** 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.

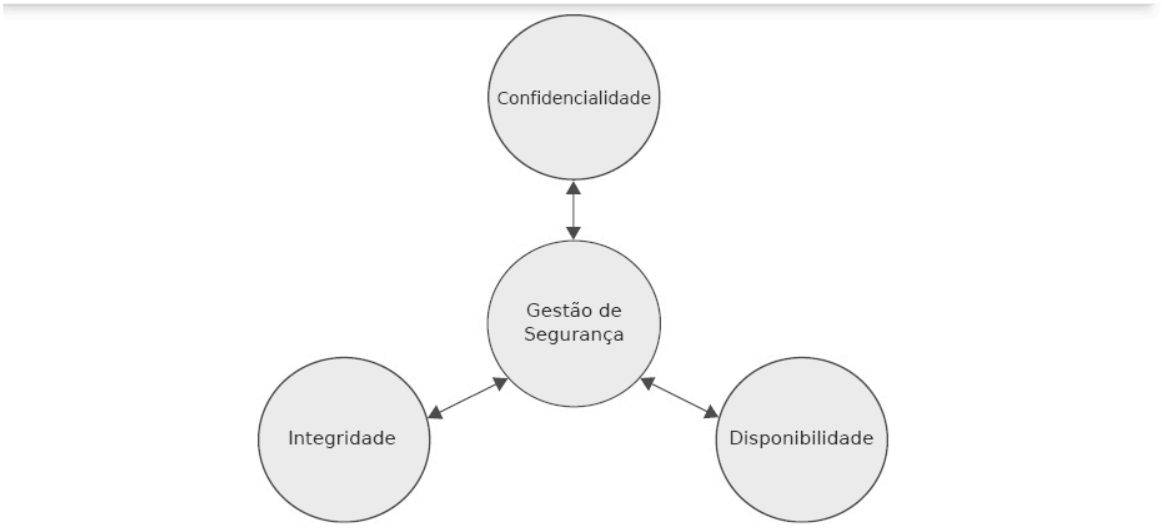
A segurança da informação é importante tanto para os negócios públicos quanto para o setor privado, e para proteger infraestruturas críticas. Em ambos os setores a segurança da informação funcionará como uma facilitadora para evitar ou reduzir os riscos relevantes.

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

3.Princípios fundamentais da Segurança da Informação

Um programa de segurança pode ter diversos objetivos, grandes e pequenos, mas os princípios mais importantes em todos os programas de segurança são a confidencialidade, integridade e disponibilidade. Estes são referidos como o triângulo CIA.

O nível de segurança requerido para executar esses princípios é diferente para cada empresa, pois cada uma tem sua própria combinação de objetivos e requisitos de negócio e de segurança. Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidas pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CIA.



Confidencialidade, integridade e disponibilidade são os princípios críticos de segurança. Você deve compreender o seu significado, como eles são providos por diferentes mecanismos e como a sua ausência pode afetar negativamente um ambiente. Tudo isso o ajuda a identificar melhor os problemas e a fornecer soluções adequadas.

3.1 Confidencialidade

A confidencialidade, também chamada de exclusividade, se refere aos limites em termos de quem pode obter que tipo de informação. A confidencialidade assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. Esse nível de confidencialidade deve prevalecer enquanto os dados residirem em sistemas e dispositivos na rede, quando forem transmitidos e quando chegarem ao seu destino.

A confidencialidade pode ser fornecida através da criptografia de dados à medida que são armazenados e transmitidos, usando preenchimento de tráfego na rede, estrito controle de acesso, classificação dos dados e treinamento de pessoal nos procedimentos apropriados.

Exemplos:

- **1.** O acesso à informação é concedido com base na necessidade de conhecer. Não é necessário que um funcionário do departamento financeiro seja capaz de ver relatórios de discussões com clientes.
- **2.** Os funcionários tomam medidas para garantir que a informação não vá para pessoas que não necessitam dela. Eles asseguram que nenhum documento confidencial seja deixado sobre suas mesas enquanto estão ausentes
- **3.** O gerenciamento de acesso lógico assegura que pessoas ou processos não autorizados não tenham acesso a sistemas automatizados, base de dados e programas. Um usuário não tem direito de alterar configurações do PC.
- **4.** É criado uma separação de funções entre a organização de desenvolvimento do sistema, a organização de processamento e a organização do usuário. O desenvolvedor não pode fazer qualquer modificação nos salários.
- **5.** São criadas separações estritas entre o ambiente de desenvolvimento, o ambiente de teste e aceitação, e o ambiente de produção.

No processamento e uso dos dados, são tomadas medidas para garantir a privacidade do pessoal e de terceiros. O departamento de Recursos Humanos pode ter sua própria unidade de rede que não é acessível a outros departamentos.

O uso de computadores por usuários finais é cercado de medidas, de forma que a confidencialidade da informação seja garantida.

As camadas de rede são criptografadas, reduzindo a oportunidade de análise do tráfego. Ainda é possível, nessas condições, um atacante acessar o volume de tráfego na rede e observar o que entra e o que sai de cada sistema final. Uma contramedida para esse tipo de ataque é o “traffic padding”.

O preenchimento de tráfego produz continuamente texto cifrado, mesmo na ausência de texto simples. Um fluxo contínuo de dados aleatórios é gerado. Quando um texto simples está disponível, ele é criptografado e transmitido. Quando não há um texto simples na entrada, dados aleatórios são criptografados e transmitidos. Isso torna impossível para um atacante distinguir entre um fluxo de dados verdadeiro e um preenchimento de dados, e, portanto, reduzir o volume de tráfego.

O preenchimento de tráfego é essencialmente uma função de criptografia de enlace. Se apenas a criptografia fim-a-fim for empregada, então as medidas disponíveis para o defensor são mais limitadas. Se a criptografia for empregada na camada de aplicação, então o oponente pode determinar a camada de transporte, o endereço da camada de rede e os padrões de tráfego, os quais permanecerão todos acessíveis.

3.2 Integridade

A integridade se refere a ser correto e consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada de dados, deliberada ou acidental, é uma violação da

integridade dos dados, por exemplo, é esperado que dados armazenados em disco sejam estáveis.

Para Donn Parker “minha definição para integridade da informação vem dos dicionários. Integridade significa que a informação é completa, perfeita e intacta. Significa que nada está faltando na informação, ela está completa e em um desejado bom estado”.

Ambientes que reforçam e fornecem esse atributo de segurança asseguram que atacantes, ou erros de usuários, não comprometam a integridade dos sistemas ou dados. Quando um atacante insere um vírus, uma bomba lógica ou um backdoor em um sistema, a integridade do sistema é comprometida. Isso pode afetar negativamente a integridade da informação contida no sistema através de corrupção, modificação maliciosa ou substituição de dados por dados incorretos. Controle de acesso restrito, detecção de intrusão e hashing podem combater essas ameaças

Os usuários normalmente afetam o sistema ou a integridade de seus dados por erro. Modificar incorretamente dados mantidos em banco de dados é outra forma comum dos usuários corromperem acidentalmente os dados, um erro que pode ter efeitos duradouros

São exemplos de medidas de integridade:

- Mudanças em sistemas e dados são autorizadas, por exemplo, um membro da equipe atribui um novo preço a um artigo no website e outro verifica a validade desse preço antes de ser publicado
- Onde possível, são criados mecanismos que forcem as pessoas a usar o termo correto
- As ações dos usuários são gravadas de forma que possa ser determinado quem modificou a informação
- Ações vitais para o sistema, como por exemplo, a instalação de software novo, não podem ser conduzidas por uma só pessoa. Ao segregar funções, posições e autoridades, ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências

A integridade dos dados pode ser garantida em grande parte por meio de técnicas de criptografia. Os princípios de política e de gestão para criptografia podem ser definidos em um documento de políticas separado

3.3 Disponibilidade

As características de disponibilidade são:

- **Oportunidade:** A informação está disponível quando necessário
- **Continuidade:** A equipe consegue continuar trabalhando no caso de falha
- **Robustez:** Existe a capacidade suficiente para permitir que toda a equipe trabalhe no sistema

Tanto uma falha de disco como um ataque de negação de serviço causam violação da disponibilidade. Qualquer atraso que exceda o nível de serviço esperado para um sistema pode ser descrito como uma violação da disponibilidade

A disponibilidade do sistema pode ser afetada pela falha de um dispositivo ou software. Dispositivos de backup devem ser utilizados para substituir rapidamente os sistemas críticos, e funcionários devem ser qualificados e estar disponíveis para fazer os ajustes necessários para restaurar o sistema. Questões ambientais também podem afetar a disponibilidade do sistema. Sistemas devem ser protegidos contra esses elementos, devidamente aterrados e monitorados de perto.

Ataques de negação de serviço (DoS) são métodos populares que hackers utilizam para interromper a disponibilidade e a utilização do sistema de uma empresa. Esses ataques são montados para impedir os usuários de acessar recursos e informações do sistema. Para se proteger desses ataques, apenas os serviços e portas necessárias devem estar disponíveis nos sistemas, e sistemas de detecção de intrusão (IDS) devem monitorar o tráfego da rede e a atividade das máquinas

Certas configurações de roteadores e firewalls também podem reduzir a ameaça de ataques DoS e possivelmente impedi-los de acontecer

Procedimentos de emergência são estabelecidos para garantir que as atividades possam ser recuperadas o mais breve possível após uma interrupção de larga escala

4.Hexadecimal Parkeriano

O hexadecimal Parkeriano é um conjunto de seis elementos da segurança da informação proposta por Donn B. Parker. O termo foi cunhado por M. E. Kabay. O hexadecimal Parkeriano soma mais três atributos aos três atributos clássicos de segurança do triângulo CIA. Em segurança da informação, um backup ou o processo de fazer backup se refere a fazer cópia dos dados de forma que essas cópias adicionais possam ser usadas para restaurar o original após um evento de perda de dados.

Os atributos do hexadecimal Parkeriano são os seguintes:

1. Confidencialidade
2. Posse ou Controle
3. Integridade
4. Autenticidade
5. Disponibilidade
6. Utilidade

Esses atributos da informação são atômicos, no sentido de que não são divididos em outras partes constituintes; não sobrepõem, já que se referem a aspectos únicos da informação.

Qualquer violação de segurança da informação pode ser descrita como aquilo que afeta um ou mais desses atributos fundamentais da informação.

5.Risco

Um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios. Se um firewall tem diversas portas abertas, há uma maior probabilidade de um invasor usar uma delas para acessar a rede de forma não autorizada. Se os usuários não forem treinados nos processos e procedimentos, haverá uma maior probabilidade de um funcionário cometer um erro, intencional ou não, que possa destruir dados. O risco amarra a vulnerabilidade, a ameaça e a probabilidade de exploração ao impacto resultante nos negócios.

Na prática:

1. Um incêndio pode surgir na sua empresa
2. Um funcionário que não trabalha no departamento de RH obtém acesso a informações sensíveis ou privadas
3. Alguém aparece como um funcionário e tenta obter informação
4. Sua empresa é atingida por uma falha de energia
5. Um hacker consegue obter acesso à rede de TI da empresa

6.Ameaça

Uma ameaça é uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização. A entidade que tira vantagem de uma vulnerabilidade é referida como agente ameaçador.

Um agente ameaçador pode ser um invasor acessando a rede através de uma porta no firewall, um processo acessando dados de uma forma que viole a política de segurança, um tornado destruindo uma instalação ou um funcionário cometendo um erro não intencional que pode expor informações confidenciais ou destruir a integridade de um arquivo.

7.Vulnerabilidade

Uma vulnerabilidade é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência ou a fraqueza de uma proteção que pode ser explorada. Essa vulnerabilidade pode ser um serviço rodando em um servidor, aplicações ou sistemas operacionais desatualizados, acesso irrestrito para entrada de chamadas no modem, uma porta aberta no firewall, uma segurança física fraca que permita a qualquer pessoa entrar em uma sala de servidores ou a não aplicação de gestão de senhas em servidores e estações de trabalho.

8.Exposição

Uma exposição é a circunstância de estar exposto às perdas provenientes de um agente ameaçador. Uma vulnerabilidade expõe uma organização a possíveis ameaças. Se a gestão de senhas for fraca e as regras para senhas não forem aplicadas, a empresa fica exposta à

possibilidade de ter a senha de usuários capturada e usada de forma não autorizada. Se uma empresa não tem seu cabeamento inspecionado e não estabelece medidas proativas de prevenção contra incêndios, ela se expõe a incêndios potencialmente devastadores.

9.Contramedida e salvaguarda

Uma contramedida é posta em prática para mitigar o risco em potencial. Ela pode ser uma configuração de software, um dispositivo de hardware ou um procedimento que elimine a vulnerabilidade ou reduza a probabilidade de um agente ameaçador ser capaz de explorar a vulnerabilidade. Exemplos de contramedidas incluem a gestão de senhas fortes, um guarda de segurança, mecanismos de controle de acesso em sistemas operacionais, a implementação de senhas da BIOS e treinamento de conscientização sobre segurança

10.Avaliando riscos de segurança - Gerenciamento de Riscos Segundo a ISO 27005

Gerenciamento de riscos é o processo de planejar, organizar, conduzir e controlar as atividades de uma organização visando minimizar os efeitos do risco sobre o capital e o lucro de uma organização.

Riscos podem surgir de vários lugares e maneiras. Diversos padrões de gerenciamento de riscos foram desenvolvidos, incluindo os do PMI (Project Management Institute), NIST (National Institute of Science and Technology) e padrões ISO. As estratégias de risco podem incluir transferir o risco para outra parte, evitar o risco, reduzir o efeito negativo do risco e aceitar algumas ou todas as consequências de um risco em particular.

Gerenciamento de riscos é um processo contínuo que se aplica a todos os aspectos dos processos operacionais. Em grandes organizações, a tarefa de monitorar esse processo é conduzida por um especialista em segurança da informação, tal como um encarregado de segurança da informação (ISO) ou um chefe de segurança da informação (CISO), que é designado especialmente para essa função é responsável pelo mais alto nível de gestão

São requisitos de segurança da informação:

1. A avaliação dos riscos à organização, levando em conta a estratégia e os objetivos globais de negócio da organização. Por meio de uma avaliação do risco, as ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o potencial impacto é estimado
2. Os requisitos legais determinados por estatutos, regulamentos e contratos que uma organização, seus parceiros comerciais, contratantes e provedores de serviço têm que satisfazer, e seu ambiente sociocultural
3. O conjunto de princípios, objetivos e requisitos de negócio para o manuseio, processamento, armazenamento, comunicação e arquivamento da informação que uma organização desenvolveu para apoiar suas operações.

Os recursos empregados na implementação de controles precisam ser equilibrados de acordo com os prejuízos de negócios que podem resultar de problemas de segurança na ausência de tais controles. O resultado da avaliação do risco irá ajudar a guiar e a determinar as ações de gestão adequadas e as prioridades para gerir os riscos.

10.1 Avaliação do Risco

Uma avaliação do risco da segurança da informação é conduzida nas primeiras etapas do projeto para identificar os controles necessários, enquanto a segurança da informação é parte de todas as fases da metodologia de projeto aplicada.

Em um mundo ideal, a segurança da informação é parte das operações diárias. Todos os funcionários estão cientes da segurança e reconhecem as falhas de segurança. A segurança da informação é implementada em todos os sistemas e um alto nível de maturidade é alcançado.

Avaliações do risco devem identificar, quantificar e priorizar os riscos segundo critérios de aceitação do risco e objetivos que são relevantes para a organização. Os resultados devem guiar e determinar as prioridades e ações de gerência adequadas para gerir os riscos de segurança da informação e implementar os controles selecionados para proteger contra esses riscos.

A avaliação do risco deve incluir uma abordagem sistemática para estimar a magnitude dos riscos e o processo de comparar o risco estimado em relação a um critério a fim de determinar a importância do risco.

As avaliações do risco também devem ser analisadas periodicamente para tratar de mudanças nos requisitos de segurança e nas situações de risco.

A avaliação do risco da segurança da informação deve ter um âmbito claramente definido, a fim de ser eficaz, e deve incluir as relações com as avaliações de risco de outras áreas, se for o caso. O âmbito de uma avaliação do risco pode ser toda a organização, partes da organização, um sistema de informação individual, componentes específicos do sistema ou serviços onde isso for viável, realista e útil.

10.2 Abordagem Sobre a Análise de Riscos Segundo a ISO 27005

O objetivo de realizar uma análise de riscos é esclarecer quais ameaças são relevantes para os processos operacionais e identificar os riscos associados. O nível de segurança apropriado, juntamente com as medidas de segurança associadas, pode então ser determinado.

Uma análise de riscos é usada para garantir que as medidas de segurança sejam implementadas de forma economicamente eficiente e oportuna, fornecendo, com isso, uma resposta eficaz às ameaças.

Segurança como um estado ou condição é a resistência a danos. De uma perspectiva objetiva, é o verdadeiro grau de resistência a danos de uma estrutura. Isso significa que o grau de resistência a danos pode variar dia após dia.

A segurança como forma de proteção é feita de estruturas e processos que fornecem ou melhoram a sensação de segurança como condição. O ISECOM (Institute for Security and Open Methodologies) define segurança como "uma forma de proteção onde é criada uma separação entre os ativos e a ameaça". Para ser seguro, ou o ativo é fisicamente removido da ameaça, ou a ameaça é fisicamente removida do ativo.

Uma análise de riscos ajuda a empresa a avaliar corretamente os riscos e a estabelecer medidas de segurança corretas e equilibradas. A administração também pode identificar os custos que estão envolvidos na adoção das medidas adequadas. Uma análise de riscos possui quatro objetivos principais:

1. Identificar os ativos e seus valores
2. Determinar os ativos e seus valores
3. Determinar o risco de as ameaças se tornarem realidade e interromperem os processos operacionais
4. Estabelecer um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança

Parte da análise de risco é uma avaliação de custo/benefício. Os custos anuais associados às medidas de segurança são comparados com as potenciais perdas que ocorreriam se as ameaças se tornassem realidade.

11.Análise Quantitativa do Risco

Uma análise quantitativa do risco tem como objetivo calcular, com base no impacto do risco, o nível de prejuízo financeiro e a probabilidade de uma ameaça se tornar um incidente. O valor de cada elemento em todos os processos operacionais é determinado. Esses valores podem ser compostos pelo custo das medidas de segurança, bem como pelo valor do próprio estabelecimento, incluindo itens como edifícios, hardware, software, informações e impacto dos negócios. Desta forma, é fornecida uma imagem clara do risco financeiro total e as medidas adequadas podem então ser determinadas.

Uma análise de riscos puramente quantitativa é praticamente impossível. Ela tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível.

12.Análise Qualitativa do Risco

Outra abordagem da análise de risco é qualitativa, e aqui números e valores monetários não são atribuídos a componentes e perdas. Ao invés disso, os métodos qualitativos caminham através de diferentes cenários de possibilidades de risco e classificam a gravidade das ameaças e a validade das possíveis contramedidas. As técnicas de análise qualitativa que podem ser utilizadas incluem bom senso, melhores práticas, intuição e experiência. Exemplos

destas técnicas são: grupos de discussão, pesquisas, questionários, listas de verificações, reuniões entre duas pessoas e entrevistas.

Quando uma equipe realiza uma análise de riscos, ela reúne pessoal com experiência e conhecimento das ameaças sobre avaliação. Este grupo é apresentado a um cenário que descreve as ameaças e as potenciais perdas, e cada membro então responde com sua intuição e experiência sobre a probabilidade da ameaça e a extensão do dano que pode resultar.

SLE, ALE, EF e ARO:

Expectativa de perda singular (SLE) é uma quantidade atribuída a um único evento, que representa a perda potencial da empresa se uma ameaça específica ocorresse: $valor\ do\ ativo\ *\ fator\ de\ exposição\ -\ EF\ =\ SLE$. O fator de exposição (EF) representa a percentagem de perda que uma ameaça ocorrida pode ter sobre certo ativo.

Expectativa de perda anual (ALE) é um valor desdobrado de suposição caso aconteça algum incidente. $ALE\ =\ SLE\ *\ ARO$.

A taxa de ocorrência anual (ARO) é o valor que representa a frequência estimada de ocorrência de uma ameaça específica dentro de um período de um ano. A faixa pode variar entre 0,0 (nunca) e 1,0 (ao menos uma vez ao ano) até valores maiores do que 1 (várias vezes ao ano).

13.ISO 27001:2013 - Mitigando os riscos à segurança

Controles de segurança são salvaguardas ou contramedidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidade devido a ameaças agindo sobre a sua correspondente vulnerabilidade. Controles são referenciados o tempo todo na segurança, mas são raramente definidos.

Antes de considerar o tratamento de um risco, a organização deve definir um critério para determinar se os riscos podem ou não ser aceitos. Um risco pode ser aceito se, por exemplo, for avaliado que o risco é baixo ou o custo do tratamento não é rentável para a organização. Tais decisões devem ser registradas. Uma decisão de tratamento de risco deve ser tomada para cada um dos riscos identificados após a avaliação de riscos. Possíveis controles para o tratamento do risco incluem:

1. Aplicar controles adequados para reduzir os riscos
2. Aceitar de forma consciente e objetiva os riscos, desde que satisfaçam claramente a política e os critérios de aceitação de risco da organização
3. Evitar riscos, não permitindo ações que possam causar a sua ocorrência
4. Transferir os riscos associados a outras partes, como seguradoras ou fornecedores
5. Ser selecionados e implementados para atender aos requisitos identificados por uma avaliação do risco

6. Assegurar que os riscos foram reduzidos a um nível aceitável levando em conta: requisitos e restrições da legislação; objetivos organizacionais; requisitos e restrições operacionais; o custo de implementação e operação em relação aos riscos sob o tratamento "redução" permanecendo proporcional às exigências e limitações da organização.

Os controles podem ser selecionados a partir da norma ISO 27002 ou de outros conjuntos de controle que a sua empresa use, ou novos controles podem ser projetados para atender às necessidades específicas da organização. É necessário reconhecer que alguns controles podem não ser aplicáveis a qualquer ambiente ou sistema de informação e podem não ser factíveis para todas as organizações.

Deve-se ter em mente que nenhum conjunto de controles consegue alcançar a segurança plena e que uma ação administrativa adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e a eficácia dos controles de segurança visando apoiar os objetivos da organização.

Quando uma ameaça se manifesta, tal como quando um hacker age para obter acesso à rede da empresa, nós chamamos isso de um incidente. Uma falha de energia, como os blecautes, é um grande incidente que pode ameaçar a sobrevivência da respectiva empresa de energia elétrica. Isso é chamado de desastre.

14.Contramedidas para mitigar o risco

A análise de riscos produz uma lista de ameaças e suas importâncias relativas. O passo seguinte é analisar cada ameaça grave e encontrar uma ou mais contramedidas que possam reduzir a ameaça. As contramedidas podem ser destinadas a: reduzir as chances de um evento acontecer; minimizar as consequências; uma combinação de ambas as coisas

Existem várias formas de definir um plano de segurança da informação e depende dos objetivos. Medidas de segurança devem sempre estar ligadas aos resultados da análise de riscos e baseadas nos aspectos de confiabilidade e características da informação. Isso pode ser dividido em seis categorias diferentes:

1. Contramedidas preventivas visam evitar incidentes

2. Contramedidas de redução visam diminuir a probabilidade de uma ameaça ocorrer

3. Contramedidas de detecção visam detectar incidentes

4. Contramedidas repressivas visam limitar um incidente

5. Contramedidas repressivas visam limitar um incidente

6. A aceitação do risco também é uma possibilidade. Dependendo do nível dos riscos, podemos também optar por aceitá-los. Uma empresa pode investir em seguros, pois decidiu que a chance de uma ameaça se tornar realidade é muito baixa para justificar o investimento em contramedidas caras

A prevenção torna impossível a ameaça ocorrer. Exemplos na segurança de TI podem incluir a desconexão de conexões com a Internet e conexões da rede local, visando assegurar que hackers externos não consigam obter acesso.

Em termos de segurança física, fechar as portas para prevenir que pessoas entrem no prédio é um exemplo, embora essa contramedida não seja muito prática. Existem outras medidas preventivas que são mais práticas.

O controle de alterações, no âmbito dos sistemas de gestão da qualidade (SGQ) e dos sistemas de tecnologia da informação (TI), é um processo formal usado para garantir que as alterações em um produto ou sistema são introduzidas de forma controlada e coordenada. O controle de alterações é um processo preventivo para reduzir a possibilidade de que alterações desnecessárias sejam introduzidas em um sistema sem premeditação. Isso também pode reduzir a possibilidade de introduzir falhas em um sistema ou desfazer mudanças feitas por outros usuários do software. Os objetivos de um procedimento de controle de alterações normalmente incluem interrupções mínimas aos serviços, redução de retrocessos e uso eficiente dos recursos envolvidos na implementação de mudanças.

Quando as consequências diretas de um incidente não são muito grandes, ou há tempo para minimizar o dano esperado, detecção pode ser uma opção. Certifique-se de que cada incidente possa ser detectado o mais cedo possível Apenas informar às pessoas que o uso da Internet é monitorado irá coibir a navegação imprópria na Internet de muitos funcionários. Uma ferramenta de monitoramento de Internet deve estar disponível para detectar o comportamento dos usuários, pois não há sentido em meramente fazer um anúncio preventivo sobre o monitoramento.

Quanto às atividades de monitoramento de rede do profissional de segurança dão uma indicação de que algo irregular aconteceu, uma ação tem que ser tomada. Quando algo realmente dá errado, isto é, quando um incidente ocorre, a coisa a ser feita é minimizar as consequências. Não há nenhuma vantagem em ter extintores de incêndio se ninguém tiver a iniciativa de usá-los em caso de incêndio. Medidas repressivas, tais como extinguir um incêndio, visam minimizar qualquer dano que possa ser causado. Fazer um backup também é um exemplo de medida repressiva. O backup pode ser usado para restaurar a última versão armazenada do documento, de forma que apenas uma parte do documento seja perdida.

Se um incidente ocorreu, sempre há algo que deve ser recuperado. A extensão do dano, seja ela pequena ou grande, depende das medidas repressivas que foram tomadas. Se um colega criar uma nova base de dados que sobrescreva a base de dados anterior, então a extensão do dano depende do backup. Quanto mais velho for o backup, maiores serão os danos produzidos.

Para eventos que não possam ser inteiramente prevenidos e para os quais as consequências não são aceitáveis, buscamos métodos que possam aliviar as consequências. Isso se chama mitigação. Seguro de incêndio nos protege contra as consequências financeiras de um

incêndio. Armazenar uma cópia de toda informação importante em um local fora da organização todos os dias garante que, no caso de um incêndio, possamos ao menos ainda ter a informação que é insubstituível. Tais medidas não são baratas, mas geralmente são consideradas justificáveis.

Quando todos os riscos necessários e conhecidos são identificados, a gerência responsável pode decidir não realizar contramedidas de segurança. Às vezes os custos não são proporcionais ao risco apresentado e ao dano que pode resultar deste. Às vezes não há contramedida adequada para mitigar a ameaça que não o risco. A contramedida reduz os riscos

15.Tipos de ameaças

Ameaças podem ser divididas em: ameaças não humanas e ameaças humanas. Para determinar as ameaças, profissionais de segurança da informação frequentemente irão se referir a listas padrões de ameaça. Essas listas são baseadas nas melhores práticas e em experiências prévias. É necessário determinar quais ameaças são relevantes e quais não são. A segurança, afinal de contas, exige que as organizações gastem dinheiro e não é sensato investir em segurança contra ameaças que não vão realmente acontecer

15.1 Ameaças humanas

Intencional: As pessoas podem intencionalmente causar danos a sistemas de informação por várias razões. Normalmente pensamos em intrusos, tais como um hacker que tem algo contra a empresa e deseja invadir e causar danos a ela. Engenharia social busca explorar a falta de consciência sobre segurança dentro de uma organização. Usar as expressões corretas ou nomes de pessoas conhecidas e seus departamentos dá a impressão de que se é um colega. Agir de forma educada e parecer confiável pode dar ao “colega” a oportunidade de obter segredos comerciais e da empresa. Um engenheiro social tira proveito dos pontos fracos das pessoas para concretizar seus objetivos. A maioria das pessoas não sabe o que é engenharia social e não reconhece um engenheiro social.

Não intencional: As pessoas também podem causar danos de forma não intencional. Por exemplo, pressionando acidentalmente o botão "delete" e confirmando de forma descuidada com OK. Além disso, em pânico, você pode usar um extintor de pó para apagar um pequeno incêndio e, de segurança, são aplicadas de maneira inadequada ou subvertida.

15.2 Ameaças não humanas

Existem também eventos não humanos que ameaçam uma organização. Estes incluem influências externas, tais como raios, incêndios, inundações e tempestades. Grande parte dos danos causados dependerá da localização do equipamento nas instalações. Podemos subdividir as ameaças humanas e não humanas em interrupções na infraestrutura básica, tais como equipamentos, software ou bases de dados computacionais, e perturbações no ambiente físico, tais como edifícios, arquivos em papel, instalações elétricas, abastecimento de água, aquecimento, ventilação e refrigeração.

16.Tipos de danos

Danos resultantes da ocorrência das ameaças citadas anteriormente podem ser classificados em dois grupos: danos diretos ou indiretos. Um exemplo de dano direto é o furto. O furto tem consequências diretas no negócio. Outro exemplo é o dano causado pela água dos extintores de incêndio. Dano indireto é a perda consequente que pode ocorrer. Um exemplo de dano indireto é ser incapaz de atender a um contrato devido à infraestrutura de TI ter sido destruída pelo fogo ou a perda de boa vontade por uma falha não intencional em cumprir as obrigações contratuais.

17.Tipos de riscos

Podemos lidar com os riscos de diferentes formas. As estratégias mais comuns são: tolerância ao risco (aceitação); redução/mitigação do risco; prevenção do risco.

Tolerância ao risco significa que certos riscos são aceitos. Isso pode acontecer porque os custos das medidas de segurança excedem o possível dano. As medidas que uma organização que tolera riscos toma na área de segurança da informação são geralmente de natureza repressiva.

Redução/mitigação do risco significa que medidas de segurança são tomadas de forma que as ameaças não mais se manifestam ou, se o fizerem, o dano resultante é minimizado. A maioria das medidas tomadas na área de segurança da informação por uma organização que neutraliza os riscos é uma combinação de medidas preventivas, de detecção e repressivas.

Prevenção do risco significa que medidas são tomadas de modo que a ameaça seja neutralizada, de tal forma que não leve mais a um incidente. Considere, por exemplo, as atualizações de software de um sistema operacional. Ao atualizar o SO assim que as atualizações estiverem disponíveis, você está prevenindo o seu sistema contra problemas técnicos conhecidos ou questões de segurança. Muitas das contramedidas nessa estratégia possuem um caráter preventivo. Independentemente da estratégia que uma organização escolhe, a administração tem que tomar uma decisão consciente e arcar com as consequências.