SEGURANÇA EM REDES DE COMPUTADORES

PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO

Autor: Me. Paulo André Zapparoli
Revisor: Rafael Rehm

INICIAR

introdução

Introdução

Apesar de o tema Segurança da Informação ganhar muita notoriedade nos últimos anos, é importante que você saiba que não surgiu recentemente. Pensando na importância para a atualidade, daremos início a esse tema, nesta unidade, começando os estudos pelos princípios básicos e fundamentais e, posteriormente, conheceremos a maturidade e um pouco da história da área de Segurança da Informação. Além disso, conheceremos normas e leis que nos auxiliam na tarefa de manter a segurança da informação, como uma das importantes diretrizes de negócios, e que nos orientam na criação de políticas e regras de segurança da informação elementos essenciais para um ambiente seguro e nos direciona a atingir os objetivos de proteção propostos.

Fundamentos de Segurança da Informação

A primeira pergunta que podemos fazer quando iniciamos os estudos nesta área é: por que se preocupar com a Segurança da Informação? Para responder a essa pergunta, é importante contextualizar o uso das redes de computadores e seus serviços. Mas, antes disso, devemos fazer duas perguntas: você consegue imaginar como procurar serviços e produtos sem o auxílio da *internet* , na atualidade? Você imagina algum serviço ou negócio que poderia funcionar, atualmente, sem utilização da rede mundial?

Provavelmente, a negativa, como resposta a qualquer uma dessas perguntas, justifique um pouco a preocupação que devemos ter com a segurança da informação. Primeiramente, precisamos perceber que a palavra segurança sempre indica que existe algum risco ao ativo que estamos associando a essa palavra, no caso, a informação que estamos buscando.

Os principais riscos ou problemas que a Segurança da Informação deve tratar são:

- Destruição de informações e outros recursos.
- Modificação ou deturpação de informações.

- Roubo, remoção ou perda da informação ou de outros recursos.
- Revelação de informações.
- Interrupção de serviços.

Como a informação é, hoje, o principal ativo de uma empresa, a segurança da informação deve ser tratada como um ponto crítico para a sobrevivência das organizações.

Princípios da Segurança da Informação

Os princípios de segurança fundamentais são a confidencialidade, a integridade e a disponibilidade. Proporcionam o foco e permitem, ao especialista de segurança, priorizar ações ao proteger qualquer sistema em rede.

A **confidencialidade** impede a divulgação de informações para pessoas, recursos ou processos não autorizados. Já a **integridade** refere-se à precisão, consistência e confiabilidade dos dados e, por fim, a **disponibilidade** garante que as informações estejam acessíveis a usuários autorizados, quando necessário. Pode-se utilizar o acrônimo CIA (do inglês), para se lembrar desses três princípios. Veremos cada um deles mais detalhadamente à frente.

O espaço digital é um domínio que contém uma quantidade considerável de dados essencialmente importantes e, portanto, é imprescindível sua proteção. Esses dados têm três possíveis estados:

- dados em trânsito;
- dados inativos ou em armazenamento;
- dados em processamento.

O trabalho de segurança da informação exige, de seus profissionais, a responsabilidade pela proteção dos dados em todos os três estágios.

No que se refere aos profissionais de segurança da informação, além de dominarem ferramentas para auxiliarem na execução de suas funções, também devem ser capazes de construir uma defesa com o estabelecimento

de políticas, procedimentos e diretrizes que orientem os usuários a ficarem seguros e seguirem as boas práticas, bem como produzir consciência e cultura de aprendizagem nesses usuários, permitindo um melhor reconhecimento de ameaças.

Confidencialidade, Integridade e Disponibilidade

A **confidencialidade** impede a divulgação de informações para pessoas, recursos ou processos não autorizados. Outro termo muito utilizado para confidencialidade é **privacidade** . As empresas restringem o acesso, para garantir que apenas os funcionários autorizados possam usar dados ou outros recursos de rede.

> *Os três conceitos envolvem os objetivos fundamentais da segurança tanto para dados quanto para serviços de informação e computação. Por exemplo, os padrões FIPS 199 (padrões para categorização de segurança para as informações e sistemas de informação federais) da NIST listam a confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informação e sistemas de informação (STALLINGS, 2015, p. 6).*

É necessário que os funcionários sejam treinados, para que tenham consciência acerca das melhores práticas sobre a proteção de informações confidenciais e, também, da organização das informações, para evitar ataques.

Há três tipos de informações confidenciais:

- *Informações pessoais:* são informações de identificação pessoal de um determinado indivíduo.
- *Informações comerciais:* são informações que incluem qualquer coisa que possa representar um risco para a empresa, se descoberta pelo público ou por um concorrente.

- *Informações confidenciais* : são informações pertencentes a um órgão do governo, classificadas pelo nível de sensibilidade.

Os métodos usados para garantir a confidencialidade incluem a criptografia, a autenticação e o controle de acesso aos dados.

A **integridade** é a precisão, a consistência e a confiabilidade dos dados durante todo o seu ciclo de vida. Outro termo para integridade é **qualidade** . Os dados passam por diversas operações, como captura, armazenamento, recuperação, atualização e transferência e devem permanecer inalterados durante todas essas operações.

A proteção da integridade de dados é um desafio constante para a maioria das empresas. A perda da integridade de dados pode tornar recursos de dados inteiros não confiáveis ou inutilizáveis.

A necessidade de integridade de dados varia, com base na maneira como a organização usa os dados. As transações e as contas de clientes devem ser precisas.

Os métodos usados para garantir a integridade de dados incluem *backups, hashing* , verificações de validação de dados, verificações de consistência dos dados e controles de acesso. Sistemas de integridade de dados podem incluir um ou mais dos métodos listados.

A **disponibilidade** dos dados é o princípio usado para descrever a necessidade de manter a disponibilidade dos sistemas e os serviços de informação o tempo todo. Ataques e falhas do sistema podem impedir o acesso a sistemas e a serviços de informação.

As pessoas usam variados sistemas de informação, diariamente. Computadores e sistemas de informação controlam a comunicação, o transporte e a fabricação de produtos. A disponibilidade contínua dos sistemas de informação é fundamental para a vida moderna. O termo “alta disponibilidade” descreve sistemas concebidos para evitar períodos de

inatividade. A alta disponibilidade garante um nível de desempenho por um período maior do que o normal. Sistemas de alta disponibilidade, normalmente, são projetados para incluírem três princípios:

- Eliminar pontos únicos de falha
- Proporcionar transição confiável
- Detectar falhas, à medida que ocorrem

O objetivo da alta disponibilidade é a capacidade de continuar a operar em condições extremas, como durante um ataque. Dentre as práticas mais populares de alta disponibilidade estão os cinco noves. Os cinco noves referem-se a 99,999%. Isso significa que o período de inatividade é menos de 5,26 minutos por ano.

reflita

Reflita

Sempre que há um ataque na rede, busca-se atingir um desses princípios citados. Exemplos: um roubo de informação afetará diretamente o princípio de ***confidencialidade*** ; derrubar um servidor afetará o princípio de ***disponibilidade*** . Reflita sobre qual ataque afetaria a ***integridade*** .

Os métodos usados para garantir a disponibilidade incluem a redundância do sistema, *backups* do sistema, maior resiliência do sistema, manutenção de equipamentos, sistemas operacionais e *software* atualizados e planos para recuperação rápida de desastres não previstos.

praticar

Vamos Praticar

Os três principais critérios de segurança da informação são confidencialidade, integridade e disponibilidade, que, juntos, formam o acrônimo (CID), muitas vezes descritos como CIA (do inglês). A respeito desses princípios de segurança da informação, assinale a afirmativa correta:

- **a)** A integridade se refere às ações tomadas para assegurar que informações confidenciais não sejam roubadas do sistema.
- **b)** Garantir a disponibilidade da informação significa que somente o usuário dono da informação poderá acessá-la.
- **c)** A confidencialidade garante a que seus servidores não serão conhecidos na internet.
- **d)** Quando o sistema tem a disponibilidade garantida com um sistema cinco noves, a integridade também estará garantida.
- **e)** A queda de seu único servidor de WEB afeta a disponibilidade desse serviço.

Gerenciamento de Segurança de TI e Avaliação de Riscos

Os profissionais de segurança precisam proteger as informações de ponta a ponta na organização. Essa é uma tarefa muito importante, e não devemos esperar que um único indivíduo tenha todo o conhecimento necessário. A Organização Internacional de Normalização (ISO) e a Comissão Eletrotécnica Internacional (IEC) desenvolveram uma estrutura abrangente para orientar o gerenciamento da segurança da informação. O modelo de segurança da ISO/IEC proporciona uma boa estrutura para entendimento e abordagem de tarefas complexas.

É com base no conjunto que o tema “Segurança da Informação” ganha muita notoriedade nos últimos anos. É importante que você saiba que não é um tema que surgiu recentemente. Apoiados nos princípios básicos e fundamentais, analisaremos o ambiente de Tecnologia da Informação. Além disso, conheceremos as documentações que nos auxiliam na tarefa de manter a segurança da informação como uma das importantes diretrizes de negócios de qualquer ramo de organização, aprendendo quais são os elementos essenciais e como atingir os objetivos por elas propostos nas normas ISO/IEC 27000, que tratam, especificamente, da Segurança da Informação, que

discutiremos os subtópicos seguintes.

Análise e Avaliação de Riscos de Segurança

O primeiro passo para criar uma proteção efetiva é saber o que devemos proteger e, depois, podemos esboçar as estratégias de segurança. A metodologia empregada para nos ajudar a obter conhecimento sobre o que proteger é a análise de risco.

O resultado da avaliação do risco é um guia que ajuda a determinar a ação de gestão e suas prioridades, bem como auxilia a implementar os controles escolhidos para proteção contra riscos e ameaças. Para manter a atualização desses controles, é necessária a repetição periódica desse procedimento.

A abordagem de processo para a gestão da segurança da informação apresentada na ISO 27002:2013 (ABNT, 2013), "Código de prática para a segurança da informação" inclui a importância de:

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

02. Gerenciar os riscos de segurança da informação da organização, implementando controles e operações no contexto dos riscos gerais de negócio da organização.

03. O Sistema de Gerenciamento da Informação deve ser constantemente monitorado e revisado, para manter o desempenho e a eficácia.

04. Melhoria contínua, baseada em medições objetivas.

Definir formas de alcançar a segurança da informação, bem como mantê-la e constantemente melhorá-la pode ser essencial para assegurar a vantagem competitiva, o fluxo de caixa, a rentabilidade, a observância da lei e a imagem comercial.

Políticas de Segurança

A política de segurança da informação necessária para uma organização, muitas vezes, é um conjunto de normas e diretrizes, que, baseada nos requisitos do negócio e nas leis e regulamentos aplicados à organização, tem o objetivo de orientar e apoiar o caminho para a segurança da informação. É necessário estar evidente, na política de segurança da informação, como gerenciar os objetivos.

> *O foco da estrutura da política de segurança de TI da sua organização é reduzir sua exposição a riscos, ameaças e vulnerabilidades. É importante relacionar a definição de política e padrões com requisitos de projeto práticos, que aplicarão corretamente os melhores controles e contramedidas de segurança. As declarações da política devem definir limites e também se referir a padrões, procedimentos e diretrizes. Políticas definem como controles e contramedidas de segurança devem ser usados para cumprir leis e regulamentações (KIM 2014, p. 31).*

Para que essa política de segurança da informação tenha força, é imprescindível a aprovação e apoio, do mais alto nível da organização.

Além disso, é importante que ela contemple, também, os requisitos oriundos da:

- estratégia de negócio;
- regulamentações, legislação e contratos;
- ameaça da segurança da informação, contemplando ambientes atual e futuro.

Para a melhor orientação do quadro de colaboradores da empresa, é importante que a política de segurança da informação contenha as seguintes declarações:

- definição da segurança da informação - apresentar os objetivos da política e os princípios que a orientam, para direcionar as atividades

relativas à segurança da informação;
- atribuição de responsabilidades (gerais e específicas) - indicar as responsabilidade pelo gerenciamento da segurança da informação e também de todos os papéis definidos dentro da política;
- processos para o tratamento dos desvios e exceções - nem centro é possível que regras gerais controlem todo o ambiente de TI, por isso, é necessário ponderar os desvios e as exceções, ao identificá-los, com regras específicas.

No nível mais baixo, convém que a política da segurança da informação seja apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e sejam estruturadas, para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

Apresentaremos, como exemplo, alguns tópicos específicos orientados aos usuários finais:

- uso aceitável dos ativos: identificados, documentados e implementados;
- mesa limpa e tela limpa;
- dispositivos móveis e trabalho remoto: garantir a segurança;
- restrições sobre o uso e instalação de *software* : definir o privilégio e quais os *softwares* são permitidos.

O conhecimento da política por todos os colaboradores e parceiros relevantes é imprescindível. Uma forma interessante para provocar isso é por meio de um programa de treinamento, conscientização e educação em segurança da informação, momento em que se detalha a política, apresentando sua relevância.

O formato adotado nos documentos que compõem as políticas de segurança da informação dependerá da estrutura da organização. Algumas empresas utilizam termos como Normas, Diretrizes ou Regras e outras podem ter em um único documento chamado "política de segurança da informação". Independentemente da nomenclatura, é crucial que tenha um ciclo que

permita sempre a revisão e novas implementações, lembrando que, para isso ser efetivo, é necessário sempre o apoio da alta direção.

praticar

Vamos Praticar

Quando o tema é segurança da informação de uma organização, logo imaginamos uma documentação organizada para esse fim, como um conjunto de normas e procedimentos que lidam com a proteção dos dados. Essa documentação é chamada de política de segurança da informação. A política de segurança tem o objetivo de mitigar os riscos e minimizar as vulnerabilidades dos sistemas de dados. As afirmações a seguir fazem referência à Política da Segurança da Informação. Assinale a alternativa correta:

- **a)** É desnecessário que a política seja aprovada pelos executivos da empresa.
- **b)** Após a criação e implantação de uma política de segurança da informação, ela será um documento inalterável.
- **c)** A política deve ser divulgada somente aos funcionários que utilizam sistemas computacionais.
- **d)** É imprescindível adotar uma forma ou programa de conscientização, educação e treinamento em segurança da informação.
- **e)** A política de segurança é um documento baseado em normas e leis, sendo assim, a política desconsidera o acesso à sua rede e a demais sistemas e plataformas tecnológicas.

Política, Controle, Planos e Procedimentos de Segurança da Informação

É muito comum ouvirmos: “A Política de Informação é uma coisa; implementá-la na organização e ver se está sendo cumprida é outra”. Se pararmos para pensar, a implementação dessa política não seria uma ação muito fácil de ser cumprida, mas também não é impossível. O primeiro passo é planejar como fazer e, depois, implementar um sistema para o gerenciamento da segurança da informação.

Plano de Segurança de TI

No planejamento, é necessário definirmos quais são as questões relevantes, externas e internas, que afetam as habilidades de alcançarmos os resultados esperados com um sistema de gerência de segurança da informação. Devemos, portanto, definir:

A. as partes interessadas, que são relevantes para o sistema de gerenciamento de segurança da informação;

B. os requisitos relevantes dessas partes interessadas para a segurança da

informação.

Para estabelecer seu escopo, a organização deve definir os limites e a aplicabilidade do sistema de gerenciamento de segurança da informação. O escopo deve estar disponível como informação documentada.

Como descrito na última revisão do texto da ISO, existe uma obrigação da organização em estabelecer, implementar, manter e promover melhorias contínuas no sistema de gerenciamento da informação, em conformidade com os requisitos dessa norma internacional.

O modelo PDCA (*plan-do-check-act* , em português, planejar-executar-checar-agir), conforme Figura 1.1, forma a base para determinar, implementar, monitorar, controlar e manter um sistema de gerenciamento da segurança da informação e pode ser o instrumento adotado nessa etapa.

> *O modelo Planejar-Executar-Checar-Agir (Plan-Do-Check-Act - PDCA), também chamado de ciclo de qualidade de Deming, forma a base para determinar, implementar, monitor, controlar e manter o sistema de gerenciamento da segurança da informação (Information Security Management System - ISMS) (HINTZBERGEN, 2015, p. 53).*

Na norma, encontraremos os requisitos para estabelecer o Sistema de Gerenciamento de Segurança da Informação (SGSI) e podemos usar o modelo PDCA, como o ciclo contínuo de melhorias do sistema:

- Planejar - como será projetado o SGSI.
- Executar - fazer a implementação do SGSI.
- Checar - verificar e acompanhar o SGSI.
- Agir - manter e aperfeiçoar, com os ajustes indicados o SGSI.

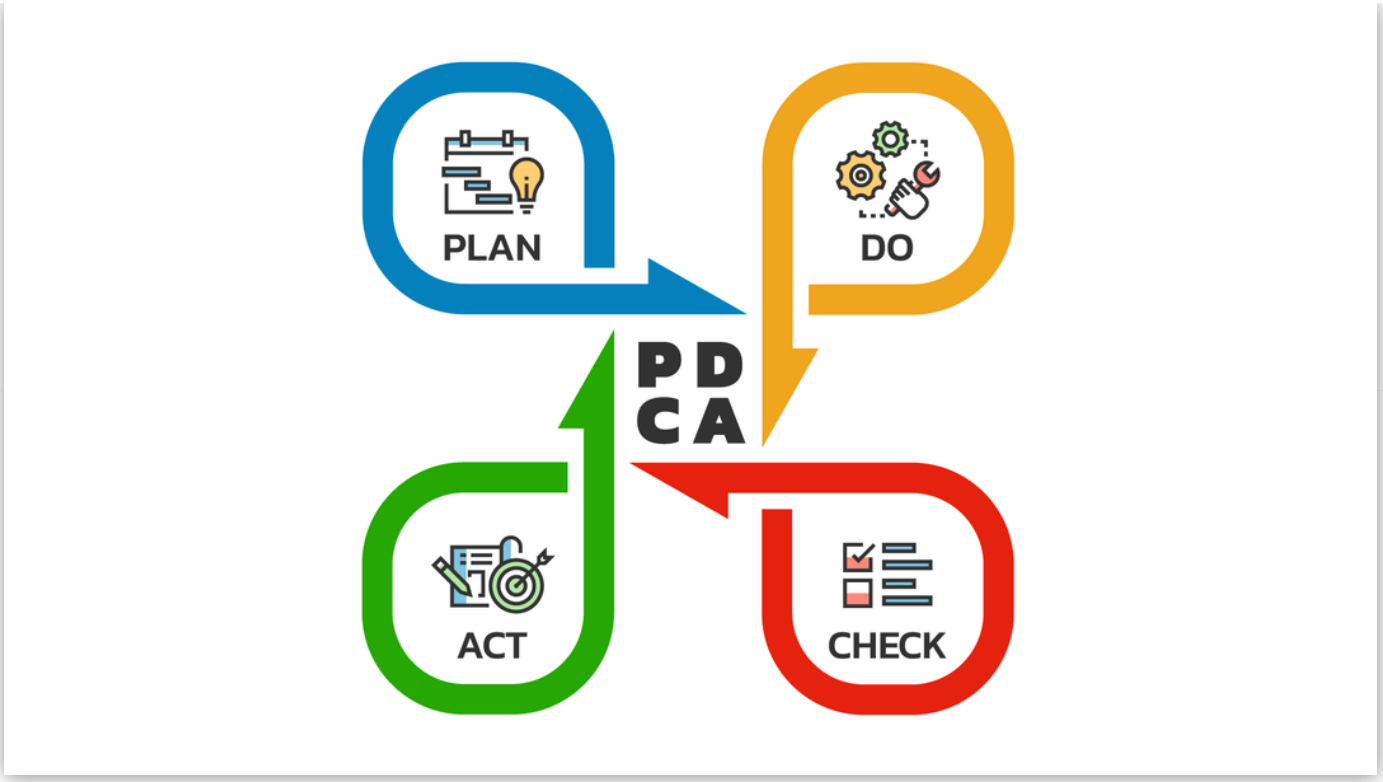


Figura 1.1 - PDCA
Fonte: Anan Punyod / 123RF.

Acompanhando as recomendações da norma ISO/IEC 27001, a organização, para estabelecer, o SGSI deve (ABNT, 2013):

A. definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo;

B. definir uma política do SGSI, nos termos das características do negócio, a organização, localização, ativos e tecnologia;

C. incluir uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas à segurança da informação;

a. considerar requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;

b. alinhar com o contexto estratégico de gestão de riscos da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer;

c. estabelecer critérios em relação a quais os riscos serão avaliados;

d. tenha sido aprovada pela direção.

D. definir a abordagem de análise/avaliação de riscos da organização.

a. Identificar uma metodologia de análise/avaliação de riscos que seja adequada ao SGSI e aos requisitos legais, regulamentares e de segurança da informação identificados para o negócio.

b. Desenvolver critérios para a aceitação de riscos e identificar os níveis aceitáveis de risco.

E. identificar os riscos;

a. Identificar os ativos dentro do escopo do SGSI e os proprietários destes ativos.

b. Identificar as ameaças a esses ativos.

c. Identificar as vulnerabilidades que podem ser exploradas pelas ameaças.

d. Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

F. analisar e avaliar os riscos;

a. avaliar os impactos para o negócio da organização, que podem resultar de falhas de segurança, levando em consideração as consequências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos.

b. Avaliar a probabilidade real da ocorrência de falhas de segurança à luz de ameaças e vulnerabilidades prevalecentes e impactos associados a esses ativos e os controles atualmente implementados.

c. Estimar os níveis de riscos.

d. Determinar se os riscos são aceitáveis ou se requerem tratamento, utilizando os critérios para aceitação de riscos.

G. identificar e avaliar as opções para o tratamento de riscos.

Possíveis ações incluem:

a. aplicar os controles apropriados;

b. aceitar os riscos consciente e objetivamente, desde que satisfaçam claramente às políticas da organização e aos critérios de aceitação de riscos;

c. evitar riscos e

d. transferir os riscos associados ao negócio a outras partes, por exemplo, a seguradoras e fornecedores.

H. Selecionar objetivos de controle e controles para o tratamento de riscos.

Objetivos de controle e controles devem ser selecionados e implementados para atenderem aos requisitos identificados pela análise/avaliação de riscos e pelo processo de tratamento de riscos. Essa seleção deve considerar os critérios para aceitação de riscos, como também os requisitos legais, regulamentares e contratuais.

Os objetivos de controle devem ser selecionados como parte desse processo, adequados para cobrirem os requisitos identificados. Controles adicionais podem também ser selecionados.

I. Obter aprovação da direção dos riscos residuais propostos.

J. Obter autorização da direção para implementar e operar o SGSI.

K. Preparar uma Declaração de Aplicabilidade, que pode incluir o seguinte:

a. os objetivos de controle e os controles selecionados e as razões para sua seleção;

b. os objetivos de controle e os controles atualmente implementados e

c. a exclusão de quaisquer objetivos de controle e a justificativa para sua exclusão.

Implementação de Gerenciamento de Segurança da Informação

As recomendações da norma ISO/IEC 27001 para a implementação de um Sistema de Gestão de Segurança da Informação são:

A. Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança.

B. Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades.

C. Implementar os controles selecionados, para atender aos objetivos de controle.

D. Definir como medir a eficácia dos controles ou grupos de controles selecionados e especificar como essas medidas devem ser usadas para avaliar a eficácia dos controles, de modo a produzir resultados comparáveis e reproduzíveis.

A medição da eficácia dos controles permite, aos gestores e à equipe, determinar o quanto os controles alcançam de forma satisfatória os objetivos de controle planejados.

E. Implementar programas de conscientização e treinamento.

F. Gerenciar as operações do SGSI.

G. Gerenciar os recursos para o SGSI.

praticar

Vamos Praticar

A ISO 27001 exige que a organização estabeleça, implemente, mantenha e melhore continuamente o sistema de gerenciamento da informação, e uma das formas de atender esse requisito é por meio do modelo PDCA. Além disso, a ISO indica, dentre outras, as seguintes definições para se estabelecer o SGSI em uma organização:

I. Analisar e avaliar os riscos.

II. Definição do SGSI pela área de Tecnologia e, assim que definido, fazer a implementação.

III. Identificar e avaliar as opções para o tratamento de riscos.

Está correto o que se afirma em:

- **a)** I e II, apenas.
- **b)** I e III, apenas.
- **c)** II e III, apenas.
- **d)** II, apenas.
- **e)** I, II e III, apenas.

Operações e Administração de Segurança

A segurança da informação é um processo contínuo. A proteção da infraestrutura da rede da organização e seus dados requer que os indivíduos permaneçam constantemente vigilantes com relação a ameaças e tomem medidas para evitar qualquer exposição ao risco.

Envolve a implementação de métodos comprovados para proteger, logicamente, os dados da organização. Alguns desses métodos envolvem a proteção do acesso administrativo, a classificação dos documentos, o conhecimento de regras e normas legais e manter-se aderente a essas regras.

Conformidade e Classificação de Dados

Para iniciarmos o trabalho de classificação de dados, precisamos entender quais dados a empresa tem, onde estão e quais são suas sensibilidades, bem como levar em consideração normas e regulamentos que regem atividades da empresa para a manutenção de suas conformidades. A partir daí, criar três ou quatro níveis de classificação de dados – não mais do que isso –, para reduzir a possibilidade de ambiguidade sobre o que cada classificação significa.

Identificar os papéis e responsabilidades na classificação de dados é importante. Devemos considerar os criadores de dados, proprietários, usuários e editores. Os dados podem ter seus níveis de classificação mudados ao longo do tempo, uma vez que progridem por meio de seu ciclo de vida ou que requisitos regulamentares evoluam.

Existem alguns critérios que devemos observar para a criação de um processo de classificação dos dados:

- Definição dos objetivos.
- Definição de critérios e categorias.
- Utilizar ferramentas de classificação selecionadas para criar os fluxos de trabalho.
- Definição dos resultados e uso de dados.

CONFORMIDADE : estar aderente aos requisitos legais e regulamentares que regem a atividade da organização.

Os registros devem ser classificados (registros de transações, registros contábeis, registros de auditoria etc.) e, conforme a categorização recebida, podem ser armazenados por mais ou menos tempo, com maior ou menor nível de segurança e em um tipo de mídia que seja mais apropriado que outro.

Gerenciamento de Mudança

No gerenciamento dos serviços de TI e também na estrutura do ITIL, existe uma orientação específica para o gerenciamento de mudanças. Conforme a norma de segurança, podemos adotar esses modelos para o gerenciamento de mudança das diretivas de segurança ou do SGSI.

saiba mais

Saiba mais

O ITIL detalha exaustivamente o gerenciamento de mudança. Reconhecimento disso é que é umas das adoções possíveis para a gestão de mudança em segurança da informação.

ACESSAR

O processo de Gerenciamento de Mudança tem os seguintes objetivos:

- responder aos requerimentos de mudanças necessárias nos serviços, maximizando valor e reduzindo incidentes, rupturas e retrabalhos;
- responder às solicitações de negócio e de TI para mudanças, alinhando os serviços às necessidades do negócio;
- assegurar que as mudanças sejam registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas e implementadas.

O Gerenciamento de Mudanças é o processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que mudanças benéficas sejam feitas com o mínimo de interrupção aos serviços de TI.

praticar

Vamos Praticar

Abordando a classificação de dados por uma perspectiva de segurança da informação, verificamos que existem alguns critérios que devemos observar para criar um processo de classificação:

I. Definir as categorias e critérios de classificação.

II. Criar fluxos de trabalho com base nas ferramentas de classificação selecionadas.

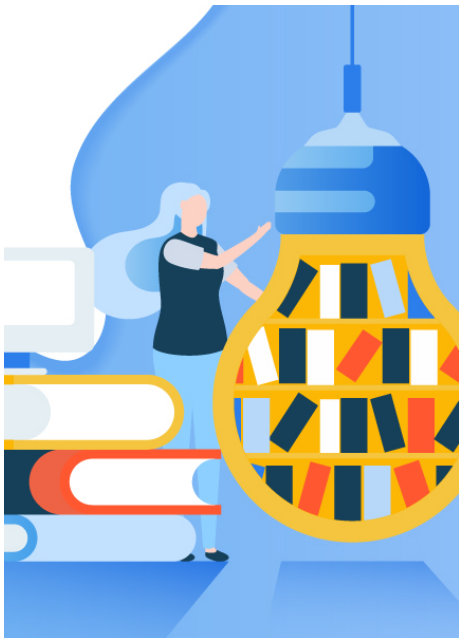
III. Definir resultados e uso de dados classificados.

Está correto o que se afirma em:

- **a)** I e II, apenas.
- **b)** I e III, apenas.
- **c)** II e III, apenas.
- **d)** II, apenas.
- **e)** I, II e III.

indicações

Material Complementar



LIVRO

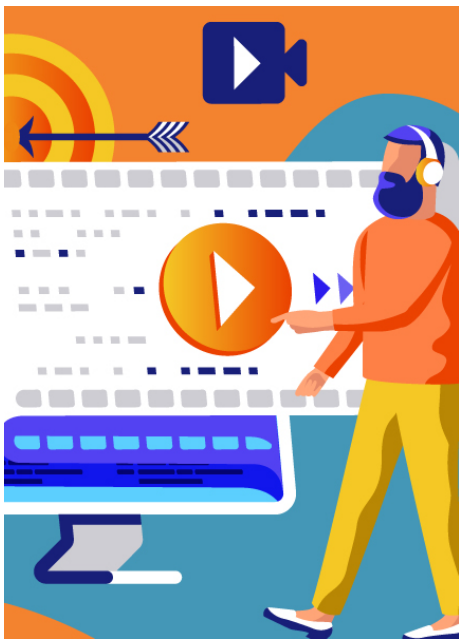
Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito

Richard A. Clarke e Robert K. Knake

Editora: BRASPORT

ISBN: 978-85-745-2711-6

Comentário: esse livro aborda a ideia das armas cibernéticas, que são usadas atualmente nas ofensivas e defesas entre Estados, por meio de ataques computacionais aos sistemas críticos, que produzem o bem-estar social e abastecimentos civil e militar. Discute, também, os impactos que essas ações podem ter na diplomacia internacional.



FILME

A Rede

Ano: 1995

Comentário: esse é um filme de ação e suspense, um dos primeiros que trata da questão de segurança e sigilosidade de informações digitais e hackeamento. Mostra como nossa vida está registrada de forma digital e quais são os possíveis impactos se o controle dessas informações for feito de forma indevida.

TRAILER

conclusão

Conclusão

Nesta unidade, conhecemos os princípios fundamentais da segurança da informação, disponibilidade, integridade e confiabilidade e sua importância para a implementação e manutenção da segurança da informação. Além disso, aprendemos sobre a análise de risco e como ela nos conduz à produção de uma Política de Segurança da Informação com as diretrizes e normas para orientar e apoiar a direção da organização e da gestão de segurança da informação no tratamento dos dados. Entendemos que uma das etapas fundamentais nessa jornada é a classificação das informações digitais, bem como a adoção de um Sistema de Gestão da Segurança da Informação.

Compreendemos, também, que a segurança da informação é processo dinâmico e, como tal, exige a implantação de um modelo de melhoria continuada, como o PDCA.

referências

Referências Bibliográficas

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001** : tecnologia da informação: técnicas de segurança: sistemas de gestão da

segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002** : tecnologia da informação: técnicas de Segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação** : com base na ISO 27001 e na ISO 27002. 3 ed. São Paulo: Brasport, 2015.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação** . Rio de Janeiro LTC, 2014.

STALLINGS, W. **Criptografia e segurança de redes** : princípios e práticas. 4. ed. São Paulo: Pearson Education do Brasil, 2015.