Princípios e conceitos de segurança cibernética

Prof. Jovair Pazzini de Melo Souza

Descrição

Introdução a princípios e conceitos de segurança cibernética no contexto da proteção de ativos da Tecnologia da Informação (TI).

Propósito

Com a evolução tecnológica dos meios de TI, aumenta-se a demanda por profissionais capacitados a enfrentarem um mundo repleto de ameaças cibernéticas constantes. Para isso, é importante que o aluno tenha contato com os principais conceitos que norteiam a segurança cibernética, com o intuito de aplicá-los em sua vida profissional.

Objetivos

Módulo 1

Evolução da segurança cibernética

Reconhecer a evolução da segurança cibernética.

Módulo 2

Alinhamento estratégico da segurança aos negócios

Reconhecer o valor da informação e o alinhamento estratégico da segurança aos negócios.

Módulo 3

Investimento necessário para garantir a proteção dos dados

Identificar o investimento necessário para garantir a proteção dos dados.

Módulo 4

Plano de cibersegurança (*Cybersecurity Plan*)

Identificar os aspectos necessários para a criação do plano de cibersegurança (*Cybersecurity Plan*).

Introdução

Em uma sociedade cada vez mais imersa no meio digital, percebemos, com maior frequência, o aumento de notícias relacionadas a incidentes cibernéticos em nosso país ou mundo afora. Com a evolução tecnológica dedicada à proteção dos ativos da Tecnologia da Informação, evoluem também as ações cibernéticas capazes de romper as barreiras dessa proteção, ou seja, qualquer sistema considerado inviolável no presente pode não ter a mesma garantia no futuro. Por essa razão, ressalta-se a importância de conhecermos mecanismos e ações relativas à área de segurança cibernética que são fundamentais para impedir ou mitigar os danos provocados pelos ataques cibernéticos.

Para isso, apresentaremos os principais conceitos relativos à segurança cibernética e sua evolução ao longo do tempo, bem como o planejamento necessário para avaliação de custos de medidas de garantia da proteção de dados em um ambiente de negócios. Por fim, abordaremos a construção do plano de cibersegurança com os principais aspectos que influenciam na garantia da proteção da informação e dos demais ativos de interesse para a segurança cibernética.

1 - Evolução da segurança cibernética

Ao final deste módulo, você será capaz de reconhecer a evolução da segurança cibernética.

Histórico da segurança cibernética

Décadas de 1970 e 1980

A evolução da tecnologia impõe uma relação de causa e efeito no contexto da segurança cibernética. Veja a seguir.

Causa	Efeito
Sempre que os meios da Tecnologia da Informação evoluem, o mesmo acontece com as ameaças cibernéticas.	Para minimizar o impacto causado por essas ameaças, são criadas e aperfeiçoadas soluções e medidas de segurança cibernética.

Nesse sentido, pode-se destacar ataques cibernéticos em grande escala, que muito contribuíram para a evolução progressiva das medidas de proteção cibernética ao longo dos anos.

> **Na década de 1970, houve os primeiros exemplos de softwares maliciosos e intrusões em computadores no contexto da ARPANET (Advanced Research Projects Agency Network), considerada precursora da atual Internet.**

Algum tempo depois, em 1983, Fred Cohen apresentou um programa capaz de copiar a si mesmo de uma máquina para outras, ao fingir ser

uma aplicação legítima para os sistemas da época. Em 1988, um massivo ataque de negação de serviço, conhecido por **DoS** (*Denial of Service*), infectou 10% de todos os computadores conectados à ARPANET. Este e incidentes anteriores motivaram países, como os Estados Unidos (EUA) e o Reino Unido, a propor e aprovar leis que definissem fraudes, abusos e a segurança em sistemas computacionais, entre 1987 e 1990.

Década de 1990

Com a criação da Rede Mundial de Computadores, *World Wide Web* (WWW), na década de 1990, a Internet é estabelecida da forma como conhecemos atualmente.

Com a popularização da Internet a nível mundial, a segurança de redes e softwares tornou-se prioridade para negócios e organizações governamentais, pois a superfície para novos ataques cibernéticos aumentou substancialmente.

Os protocolos criados para a Internet foram pensados prioritariamente de forma a garantir a usabilidade, mas não a segurança. Dessa forma, ataques como o worm **Melissa**, o qual infectou centenas de computadores ao redor do mundo e causou falhas em servidores de e-mail, começaram a se tornar mais frequentes, motivando ainda mais a busca por soluções de cibersegurança mais amplas e eficazes.

Anos 2000

No ano de 2000, havia mais de 300 milhões de usuários conectados à Internet. A utilização massiva da rede aumentou as probabilidades para ataques maiores, como o worm **"ILOVEYOU"**. Esse artefato malicioso infectou 50 milhões de sistemas ao redor do mundo em apenas dez dias.

Em 2001, para estabelecer um entendimento sobre crimes cometidos por meio da Internet, o Conselho da Europa reuniu-se durante a Convenção sobre Crimes Cibernéticos e propôs a assinatura de um tratado sobre o tema. Com o aval de mais de 60 países, o tratado foi ratificado.

Em 2002, a União Europeia adotou uma política de proteção aos dados confidenciais em meio eletrônico e, em 2003, os Estados Unidos criaram sua Divisão Nacional de Segurança Cibernética.

Entre 2010 e 2022

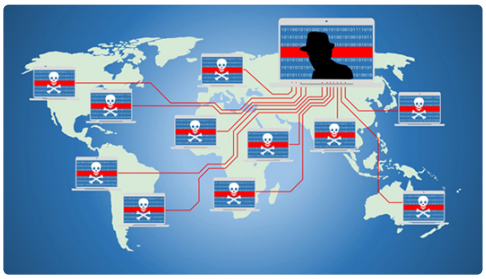
Ao longo dessa década, o número de dispositivos eletrônicos continuou a crescer, com a adoção de equipamentos de controle de automação e de sistemas, além da gigantesca quantidade de dados vista no fenômeno da **Big Data** e da ascensão da **Inteligência Artificial**. Esses fatos trouxeram novos desafios para a Segurança Cibernética, como visto em incidentes ao longo da década, quando houve inúmeros ataques cibernéticos que causaram o vazamento de dados pessoais de milhões de usuários, inclusive dados bancários.

Ataques por **ransomwares** e **botnets**, ilustrados pelo WannaCry e Mirai, respectivamente, revestiam-se de aprimoramentos consideráveis comparando-se com tipos de malwares anteriores.

Veja a seguir como atua cada um desses tipos de malware.

Ransomware

É utilizado por cibercriminosos para criptografia dos dados pessoais do usuário e, mediante resgate financeiro, geralmente em criptomoedas, oferecem a chave criptográfica para que o usuário recupere seus dados.



Botnet

Atua infectando dispositivos para controlá-los remotamente e, a partir desses dispositivos, executa Ataques de Negação Distribuída de Serviço (DDoS) para comprometer outros alvos.

Esses dois tipos de malware, ao se aproveitarem de uma quantidade gigantesca de usuários com dispositivos vulneráveis conectados à Internet, foram responsáveis por causar danos econômicos consideráveis a vários indivíduos e organizações.

Como se não bastasse o impacto visto em ataques anteriores, outras ameaças como a *Advanced Persistent Threat* (APT), ou em português **Ameaça Persistente Avançada**, demonstraram que o nível de elaboração de ataques cibernéticos não havia chegado ao seu limite. Tão avançada quanto ransomwares ou botnets, uma **APT** dispõe de técnicas que encobrem rastros de cibercriminosos e, mesmo parecendo que as medidas de segurança como antivírus ou firewall tenham contido essa ameaça, geralmente são deixadas brechas para um possível acesso futuro pelos criminosos.

Geralmente, o alvo de APTs inclui até instituições de outros países. Nesse contexto, esse e outros tipos de ameaças cibernéticas podem ser identificadas como armas cibernéticas, como no caso do malware Stuxnet, que causou impactos severos no programa nuclear do Irã ao inutilizar centrífugas de enriquecimento de urânio. Esse e outros ataques ocorridos inserem-se no contexto da denominada Guerra Cibernética, a qual é reconhecida como uma dimensão adicional do combate moderno ao impulsionar a tensão geopolítica entre nações.

Comentário

Paralelamente a esses ataques, há uma preocupação de vários países para que a privacidade de dados sensíveis dos usuários não seja comprometida, o que induziu à criação de políticas de proteção de dados como General Data Protection Regulation (**GDPR**), Network Information and Security (**NIS**) e European Cybersecurity Act.

Ao vislumbrarmos a diversidade de ataques cibernéticos ao longo de mais de cinquenta anos, de forma geral, podemos dizer que as medidas de Segurança Cibernética evoluíram consideravelmente com a criação de novas tecnologias, como **firewall, antivírus e sistemas de detecção, intrusão** e **mitigação de ameaças**. Com isso, percebe-se que, dado o prejuízo financeiro causado pelo maior alcance e pela sofisticação de ataques cibernéticos, houve um esforço no sentido de desenvolver medidas de prevenção às ameaças, muitas vezes com o auxílio da Inteligência Artificial.

Segurança cibernética e da informação

Conceitos

Há várias definições para o conceito de segurança cibernética, dada a extensão e complexidade dos fatos que embasaram sua evolução, porém, de forma geral, podemos defini-la como:

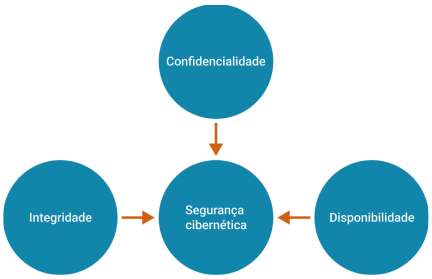
> **Segurança cibernética – conjunto de medidas responsáveis por preservar a confidencialidade, integridade e disponibilidade da informação no ciberespaço. Podemos definir ciberespaço, ou espaço**

> **cibernético, como um ambiente complexo resultante da interação de pessoas, softwares e serviços na Internet disponíveis em dispositivos de tecnologia e redes conectadas entre si.**

Tal conceito é similar ao de Segurança da Informação, definido por:

> **Segurança da informação – conceito mais abrangente que a segurança cibernética, pois assegura o acrônimo CID (confidencialidade, integridade e disponibilidade) da informação em qualquer meio, quer esteja no ciberespaço ou não.**

Para exemplificar a diferença entre esses dois conceitos, podemos dizer que, se há uma carta com informações sobre local e hora de uma reunião confidencial, essa pode não ser considerada um ativo de interesse para a segurança cibernética, mas para segurança da informação, sim. Por outro lado, qualquer informação confidencial armazenada em ativos de TI, como computadores, laptops, servidores, dentre outros, torna-se alvo de proteção tanto para a segurança cibernética quanto para a segurança da informação.



Pilares da segurança cibernética.

Podemos definir os pilares demonstrados na imagem anterior da seguinte forma:

Disponibilidade

Garante que, quando necessário, um sistema de informação ou de serviços de segurança esteja sempre em funcionamento e acessível quando demandados por uma entidade autorizada.

Exemplo: um site de uma rede social encontra-se em funcionamento 24 horas por dia, porém, se um ataque cibernético faz com que o site fique off-line, podemos dizer que a disponibilidade das informações do site foi afetada.

Confidencialidade

Garante que a informação seja revelada apenas a indivíduos, entidades ou processos autorizados.

Exemplo: ao enviarmos um e-mail para um ou mais indivíduos específicos, o resultado esperado é que apenas os destinatários de interesse recebam a informação, garantindo a confidencialidade.

Integridade

Garante a completa composição da informação, sem qualquer tipo de alteração, por menor que seja, realizada por entidades não autorizadas.

Exemplo: um arquivo com uma apresentação de negócios teve seu conteúdo alterado ao ser manipulado por outra pessoa. Como consequência, a integridade do arquivo foi violada, pois as informações nele foram modificadas.

Propriedades adicionais da segurança cibernética

Assim como na segurança da informação, pilares adicionais como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidos no contexto da segurança cibernética. De forma a explicá-los com maior clareza, podemos defini-los da seguinte maneira:

Autenticidade

É o pilar que permite a comprovação verídica da autoria ou origem de determinada informação. Exemplo: a assinatura digital de um indivíduo permite atestar a ligação entre ele e a informação por ele produzida.

Não repúdio

É o pilar em que não é possível negar a autenticidade da informação. Exemplo: a assinatura digital descrita no exemplo anterior não permite que o próprio autor ou terceiros refutem a autoria da informação.

Responsabilidade

É o pilar que atribui ações e decisões a um indivíduo em relação à informação. Exemplo: um profissional de uma empresa é responsável pela segurança das informações pessoais dos clientes, no entanto, por descuido, envia para um colega um

arquivo contendo todas essas informações. Nesse caso, o pilar da responsabilidade obriga-o a responder por esse ato.

Confiabilidade

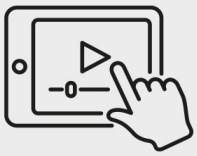
É a propriedade verificada quando a informação é consistente e apresenta comportamento e resultado desejados. Exemplo: quando alguns dos pilares anteriores não são assegurados, incluindo os da disponibilidade, confidencialidade e integridade, podemos dizer que a confiabilidade da informação foi afetada.

Você acabou de ver como esses pilares são importantes para a segurança cibernética.

Grandes ataques cibernéticos

Veja a seguir uma abordagem dos principais ataques cibernéticos ocorridos no século passado e atual e quais impactos essas ameaças trouxeram no processo de evolução da tecnologia para a criação de medidas de segurança cibernética eficazes.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Uma empresa utiliza um sistema de impressoras em rede, compartilhado por vários funcionários, porém, ao deslocar-se para coletar seu relatório semanal de atividades na impressora compartilhada, um dos funcionários do setor Financeiro percebeu que havia outro documento com informações restritas ao setor de Relações Humanas (RH). Diante desse fato, qual das propriedades da informação listadas abaixo foi violada?

A Não repúdio

B Integridade

C Disponibilidade

D Confidencialidade

E Autenticidade

Parabéns! A alternativa D está correta.

Por ser um documento restrito ao setor de Relações Humanas, outros funcionários não deveriam ter acesso ao seu conteúdo; logo, a confidencialidade das informações do documento foi violada, pois qualquer pessoa ou entidade sem autorização poderia lê-lo.

Questão 2

Um hacker obtém acesso à caixa de e-mail de um dos funcionários de uma empresa. Após isso, ao se passar pelo detentor do e-mail, começa a enviar mensagens para centenas de funcionários. Em seu conteúdo, o e-mail enviado possui um link para o download de um suposto relatório de produtividade da empresa, o qual, na verdade, é um malware. Esse artefato malicioso, ao ser executado, concede acesso remoto do computador alvo ao hacker. Diante do fato, em relação aos aspectos da informação listados abaixo e suas respectivas justificativas, qual deles foi violado?

A Disponibilidade, pois o e-mail encontra-se indisponível para funcionários que não receberam o e-mail.

B Não repúdio, pois é impossível negar a autoria do e-mail.

C Integridade, pois o e-mail enviado não é íntegro.

D Confidencialidade, pois o e-mail foi enviado para muitos funcionários.

E Autenticidade, pois, ao fingir ser o funcionário, o hacker altera a original autoria do e-mail.

Parabéns! A alternativa E está correta.

A alteração de forma indevida da autoria da informação, ou mesmo a inviabilização de comprovação da origem, viola a autenticidade do conteúdo de qualquer informação. No caso em questão, um e-mail foi disparado por um hacker disfarçado de legítimo funcionário da empresa.

2 - Alinhamento estratégico da segurança aos negócios

Ao final deste módulo, você será capaz de reconhecer o valor da informação e o alinhamento estratégico da segurança aos negócios.

Informação e dado

Conceitos

O conceito de **dado** está intrinsecamente associado ao conceito de **informação**. Veja como ocorre a relação entre eles.

Dado	Informação
É o elemento desprovido de significados.	É o resultado do elemento após passar por processos de organização, manipulação, análise e avaliação.

Isso ocorre porque os dados, elementos desprovidos de significado, após passarem pelo processo de organização, manipulação, análise e avaliação, adquirem a característica de informação.

Desse modo, é basilar que o profissional de cibersegurança identifique em quais ativos a informação poderá estar. Cada formato e ativo pode exigir abordagens diferentes de medidas de segurança, lembrando que a informação poderá estar em vários formatos como texto, vídeo, áudio, dentre outros.

Em um contexto mais amplo, não importando o ativo de TI em que a informação possa residir, sabe-se que os dados podem ser agregados de acordo com a finalidade do Sistema de Informação (SI) a qual pertencem.

> **O SI possui a tarefa de reunir, armazenar, processar e distribuir informações relevantes para clientes, funcionários e gestores.**

No contexto da segurança cibernética, os SI podem estar em diferentes ativos conectados ao meio cibernético, como:

- Data centers;
- Estações de trabalho;
- Computadores pessoais;
- Discos;
- Impressoras;
- Sistemas operativos e outros.

Além disso, os **SI** podem auxiliar a empresa no processamento de suas transações, no apoio à decisão e na automação de tarefas, por exemplo. Cada organização poderá apresentar tecnologias diferentes para cada SI, mas, mesmo assim, a metodologia das ações para proteção de cada sistema será a mesma.

A proteção de dados é o primeiro passo para garantir a segurança das informações de uma organização. Por mais que os dados sejam elementos aparentemente sem significado, ainda assim podem fornecer o entendimento de informações críticas e sensíveis para uma organização.

Exemplo

Vários bancos de dados podem conter itens como: nome, sobrenome, estado civil, ano de nascimento, local de nascimento, dentre outros itens afins. Suponhamos que, em um desses bancos de dados, encontram-se estes dados pessoais: Sara Ferreira, solteira, 2001 e Rio de Janeiro-RJ. Qual informação é possível abstrair desses elementos? Provavelmente, poderíamos dizer que a Srta. Sara Ferreira nasceu na capital do estado do Rio de Janeiro no ano de 2001.

O exemplo apresentado foi apenas um dos que podemos encontrar no cotidiano das atividades de negócios das organizações.

A informação é considerada um dos fatores de produção, ao lado de fatores como o capital, o trabalho e a matéria-prima. Por essa razão, no meio corporativo, não é incomum ouvirmos frases como “informação é poder”. Basta visualizarmos casos reais em que empresas desprovidas de informações podem se tornar inoperantes ou menos competitivas em relação a outras do mesmo ramo.

A classificação da informação

Fatores

Importante passo para **proteção dos dados** e, como consequência, das informações, a etapa de classificação da informação sustenta-se em critérios descritos nos manuais de boas práticas e normatizações, como a **ISO** (International Standards Organization) e a **NIST** (National Institute of Standards and Technology). Essas instituições orientam a catalogação da informação de acordo com seu risco e sua criticidade, dada sua importância em diferentes níveis para a organização a qual pertença.

Observe os critérios utilizados em uma organização para classificar a informação:

• **Sensibilidade**: normalmente o nível de sensibilidade dos dados pode ser ultrassecreto, secreto, confidencial, restrito ou público. Um exemplo seria o telefone da ouvidoria de uma empresa em um site na internet, pois tal informação pode ser considerada pública, diferentemente dos dados particulares das pessoas que ligam para reclamar do atendimento dessa empresa, os quais normalmente não são considerados dados públicos, mas sim restritos com algum grau maior ou menor de sensibilidade;

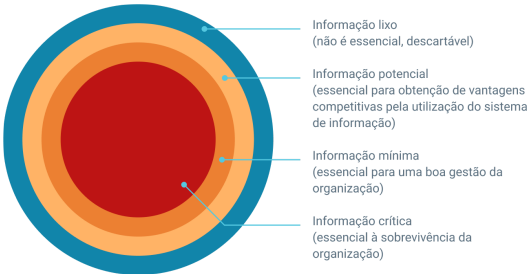
• **Valor**: é variável, ou seja, alguns indivíduos podem ter interesse em um dado ou uma informação, enquanto esse dado ou essa informação pode não fazer diferença para outros. Para garantir a segurança da informação, a atribuição de valor surge como uma medida eficaz para otimização de tempo e recursos gastos;

• **Requisitos legais**: é o ordenamento jurídico do local onde se encontra a organização. Por exemplo, com relação à privacidade dos dados, se a organização se encontra no Brasil, então estará sujeita ao regulamento jurídico imposto pela Lei Geral de Proteção de Dados (LGPD);

• **Importância**: assim como no caso da quantificação do

valor, mensurar o quão relevante a informação é para o funcionamento de determinada organização também evita gastos desnecessários de recursos e tempo.

Ainda sobre a informação, ela pode ser classificada em: informação **crítica**/ informação **mínima**/ informação **potencial** e informação **lixo**, conforme mostra a imagem a seguir.



Classificação da importância da informação.

Nota-se que as informações devem passar por um filtro para análise do grau de importância, pois nem todas são relevantes para o funcionamento de uma organização. À medida que são filtradas, entende-se o papel que cada informação desempenha no contexto da organização da qual faz parte. Naturalmente, algumas informações serão totalmente irrelevantes, assim como outras serão indispensáveis para o gerenciamento das atividades de negócios.

A classificação da importância da informação leva em consideração dois princípios:

Presença da informação

Neste caso, a organização já possui a informação, logo, a importância é medida pelos custos relacionados à sua obtenção, manutenção e utilização.

Ausência da informação

Aqui, se a informação é necessária para a organização, mas não obtida, sua importância é calculada com base no custo da oportunidade de sua ausência, ou seja, a organização arca com o custo de não ter informações necessárias para utilização em benefício próprio.

O valor da informação

A Importância do Valor

Vimos que o valor é um dos aspectos levados em consideração para auxiliar no processo de garantia da segurança da informação. Por ser de extrema relevância no processo de classificação da informação, divide-se em 4 (quatro) tipos:

Valor de uso

É definido pelas vantagens proporcionadas pelo uso da informação, de acordo com finalidade compatível.

Exemplo: uma informação sobre qual o modelo de carro mais desejado pelos moradores de uma cidade pode beneficiar uma concessionária de revendas. O lucro final obtido pela concessionária, após vender os carros de modelo correspondente ao da informação, representará o valor de uso.

Valor de troca

É definido pelo quanto um usuário está disposto a pagar por determinada informação, podendo ser maior, igual ou menor que o valor de uso.

Exemplo: uma empresa de consultoria financeira pode fornecer informações sobre o mercado de ações na bolsa de valores. Digamos que o valor pago para ter conhecimento de quais ações irão se valorizar seja de X reais, no entanto, o lucro proveniente de tais ações, o qual é definido pelo valor de uso, pode ser maior ou menor que X, ou até mesmo igual.

Valor de propriedade

Ocorre quando o valor da informação é determinado pelo seu proprietário, não refletindo exatamente o mesmo valor de troca ou de uso.

Exemplo: informações sobre o gênero de filme mais visto em uma plataforma de streaming de uma empresa podem não ter o mesmo valor para uma plataforma de transporte de encomendas.

Valor de restrição

É identificado em informações secretas ou que possuam determinado grau de interesse comercial. Tal valor determina a frequência de utilização da informação, podendo ser mais ou menos restrito seu uso.

Exemplo: informações sobre investigações policiais em casos de homicídio, ou sobre produtos inéditos em processo de desenvolvimento.

A correta classificação do valor da informação pode ser caracterizada como fato propulsor para o sucesso nos negócios de uma organização, além de auxiliar no processo de tomada de decisões, pois, em tese, a classificação de informações pode ajudar uma empresa a identificar as informações mais valiosas, que poderão aumentar os ganhos e minimizar as perdas.

A classificação da informação nos ativos de TI

Procedimentos

Percebe-se que há uma subjetividade inserida nos fatores que influenciam o processo de classificação da informação. Organizações possuem peculiaridades que implicam a existência de informações com maior ou menor sensibilidade. Para realizar a classificação do grau de sensibilidade da informação, seguimos estas ações:

Categorizar a informação

É a ação na qual designa-se um indivíduo ou grupo de pessoas a terem acesso às informações de acordo com sua função na hierarquia da organização ou de acordo com a relação que possuem com assuntos específicos.

Atribuir dono para o ativo de TI

É a ação na qual determina-se um indivíduo responsável pelo eventual acesso à informação por outros indivíduos. O detentor direto do ativo de TI não poderá ser o dono, pois este tem a autoridade sobre as informações e como são acessadas, já o detentor possui apenas a responsabilidade diária pela integridade do material.

Etiquetar as informações

De acordo com a constituição do ativo de TI, seja ele físico ou digital, e com a sensibilidade das informações armazenadas nos ativos, poderá ser realizada uma classificação com etiquetas em partes do material, como em cabos ou em monitores, por exemplo. Se o ativo for digital, a classificação poderá ser atribuída no conteúdo do arquivo, como no caso de um arquivo de texto, em que a etiqueta de "confidencial" ou "restrito", por exemplo, poderá vir no cabeçalho e/ou rodapé de cada página.

Em relação aos procedimentos apresentados, pode-se argumentar como seriam aplicados em uma organização.

Exemplo

Digamos que há uma pasta compartilhada em rede, na qual residem vários arquivos com dados sigilosos sobre um projeto dedicado à criação de um novo modelo de produto. Sabe-se que a pasta em rede precisa ser acessada por outros funcionários. Para isso, o funcionário que deseja o acesso deve solicitar a permissão ao dono, o qual deve possuir responsabilidade por aqueles que têm acesso aos arquivos.

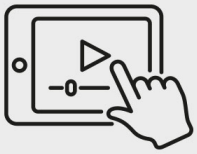
O dono deverá verificar se o integrante da empresa que solicitou o acesso possui relação com o assunto e as informações existentes na pasta em rede. Além disso, deverá ser levado em consideração o nível de sensibilidade do assunto, pois os arquivos dentro da pasta compartilhada podem possuir etiquetação com maior ou menor restrição. Pode haver arquivos confidenciais, secretos ou com qualquer outro nível, a ser definido pelo dono do ativo. Somente após todos esses procedimentos de verificação, é que o membro da organização poderá ter acesso garantido às informações da pasta compartilhada.

No entanto, cuidado para não confundir Dado com Informação, pois apesar de estarem relacionados, possuem significados distintos.

Dado e informação

Veja a seguir uma abordagem dos conceitos referentes a dado e informação e exemplos de cada conceito.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

John Doe, especialista de Segurança Cibernética de uma empresa, recebeu a missão de classificar as informações contidas nos servidores que armazenam arquivos relacionados aos processos de inovação de aplicativos para celulares. Ao analisar os arquivos, deparou-se com diversos tipos de projetos inéditos em relação a empresas no mesmo ramo do mercado atual de aplicativos e decidiu classificar como ultrassecretas as informações contidas em tais projetos. Diante dessa situação, qual dos fatores abaixo foi levado em consideração para aplicação da classificação das informações feita por John?

A — Requisitos legais, pois as informações deveriam estar classificadas de acordo com a legislação do país vigente.

B — Valor, pois as informações, no contexto apresentado, possuem altíssimo valor comercial agregado.

C — Sensibilidade, pois diz respeito ao maior ou menor grau em que uma organização pode considerar uma informação restrita ou pública.

D — Importância, pois as informações possuem alto nível de criticidade para a sobrevivência da empresa.

E — Prioridade, pois tal informação claramente possui prioridade de segurança em detrimento de outras.

Parabéns! A alternativa C está correta.

A classificação da informação como ultrassecreta diz respeito à sensibilidade, pois as informações de uma organização podem ser públicas ou restritas. Se a informação sobre criação de aplicativos fosse pública ou pouco restringida, um número maior de pessoas teria acesso, diminuindo o sigilo da informação e causando

possíveis prejuízos se as informações sobre os projetos fossem divulgadas para empresas concorrentes, por exemplo.

Questão 2

Alice é especialista em Segurança Cibernética e está classificando uma série de informações importantes para a empresa em que trabalha. Ao iniciar a classificação dos dados na Seção de Relações Humanas, percebeu que havia dados como nome completo, CPF, RG, endereço, agência e conta bancária de todos os funcionários da empresa, além de que todos esses dados estavam armazenados em uma pasta compartilhada em rede.

O processo operacional da empresa delega exclusivamente ao Chefe da Seção de RH a função para inserir, alterar e excluir informações sobre os funcionários novos, atuais ou os que já deixaram a empresa, porém outros funcionários da seção têm acesso às informações, só podendo realizar alguma alteração com a autorização expressa do chefe da Seção de RH.

Levando-se em consideração os procedimentos e fatores para a classificação da informação nos ativos de TI, assinale a opção que representa as ações recomendadas para que Alice classifique as informações de acordo com a situação apresentada.

A	Permitir que toda Seção de RH tenha acesso à pasta, mas apenas o chefe possa fazer alterações; designar o chefe da Seção de RH como dono da pasta compartilhada e etiquetar as informações pessoais dos funcionários como públicas.
B	Permitir que toda a Seção de RH tenha acesso à pasta, mas apenas o Chefe possa fazer alterações; designar o chefe da Seção de RH como dono da pasta compartilhada e etiquetar as informações dos funcionários como restritas.
C	Permitir que toda a Seção de RH possa fazer alterações nas informações dos arquivos, designar todos os funcionários da Seção de RH como donos da pasta e etiquetar as informações dos funcionários como restritas.
D	Permitir que apenas o chefe da Seção de RH tenha acesso à pasta, designá-lo como dono da pasta compartilhada e etiquetar as informações dos funcionários como públicas.

E	Permitir que toda a Seção de RH possa fazer alterações nas informações dos arquivos, designar o chefe da Seção de RH como dono da pasta compartilhada e etiquetar as informações dos funcionários como públicas.

Parabéns! A alternativa B está correta.

Pela linha de raciocínio do enunciado, o chefe da Seção de RH deveria ter acesso e poder de modificação dos dados. Os demais funcionários da seção poderiam ter apenas o acesso. Por essa razão, a fim de ser realizado esse controle, o chefe deveria ser designado como dono do ativo para que possa auditar o acesso dos funcionários à pasta compartilhada. Em relação à sensibilidade da informação, por se tratar de informações pessoais e sensíveis, o ideal é que fossem classificadas como restritas.

3 - Investimento necessário para garantir a proteção dos dados

Ao final deste módulo, você será capaz de identificar o investimento necessário para garantir a proteção dos dados.

Gerenciamento de riscos para a proteção de dados

Requisitos

No contexto da segurança cibernética, a proteção de dados pode envolver vários tipos de medidas de segurança. Por esse motivo, é imprescindível considerar o fator principal envolvido no cálculo do investimento necessário para a devida proteção dos dados de uma

organização: o **risco**, ou a **vulnerabilidade**. Veja a seguir as características desses fatores.

Risco

O risco à segurança da informação e cibernética é a probabilidade de ameaças explorarem com sucesso vulnerabilidades existentes em ativos, representando um dano potencial à organização em que se inserem.

Vulnerabilidade

Ela pode ser representada pela fraqueza em um ativo. Caso a vulnerabilidade seja de alguma forma explorada pela ameaça, denominamos esse acontecimento como **incidente**.

O correto gerenciamento de risco é imperativo para que se determine a quantidade de recursos a ser gasta com medidas viáveis e indispensáveis para que se evitem incidentes cibernéticos. Um incidente cibernético pode ocorrer quando hackers agem para obtenção de acesso à rede corporativa de uma empresa ou instituição pública, por exemplo.

A **eficácia** é um importante fator a ser levado em consideração no momento de adoção de medidas de segurança, porém muitas vezes tais medidas apresentam valores de investimento elevados, inviáveis para muitas organizações que não possuem dados tão valiosos ou tão críticos assim, ou mesmo não possuem capital necessário para esse investimento. O recomendável é que seja estimado um valor para cada ativo inserido no contexto da Segurança da Informação e, após isso, deve-se verificar se os custos de medidas de segurança são iguais, inferiores ou maiores do que o ativo a ser protegido.

Em relação à **natureza dos riscos**, muitos deles poderão estar associados a incertezas do mercado financeiro, acidentes naturais ou desastres, ataques cibernéticos, dentre outros identificados por uma organização. Cabe lembrar que o risco é algo incerto, porém, se houver um processo de gerenciamento de riscos internamente por cada organização, pode ser previsto e minimizado.

O **gerenciamento de risco** é uma atividade contínua aplicada a todos os processos operacionais de uma operação, conduzida pelo Encarregado de Segurança da Informação ou pelo Chefe da Segurança da Informação, o qual deve atentar-se para os três principais requisitos:

1. **Realização da avaliação de riscos** levando-se em consideração a estratégia de negócios da organização, bem como as ameaças aos ativos, vulnerabilidades encontradas, probabilidade de concretização do risco e uma estimativa do potencial impacto.

2

Requisitos legais, previamente determinados por contratos, regulamentos e estatutos, os quais são seguidos pela organização, contratantes, parceiros comerciais e provedores de serviço, além do ambiente sociocultural em que se encontram.

3

Conjunto de objetivos, requisitos e princípios de negócios utilizados para armazenamento, processamento, manuseio, comunicação e arquivamento da informação que organizações desenvolvem para apoio em suas decisões.

Um dos aspectos essenciais para o correto gerenciamento de risco é o cálculo estimado do prejuízo financeiro se os controles de segurança contra os riscos não forem implementados. Em outras palavras, deve-se avaliar os prejuízos decorrentes da não adoção de eventuais medidas relevantes para a proteção de dados da organização.

Análise e avaliação de riscos

Objetivos

A **análise e a avaliação de riscos**, atividades inseridas no contexto do processo de gerenciamento de riscos, podem ser aplicadas em toda a estrutura da organização, em partes dela, bem como em componentes específicos de sistemas e serviços. Essas atividades, mesmo para especialistas mais experientes, requerem um alto nível de compreensão para diferenciação de medidas de segurança, muitas vezes ineficazes ou não adequadas, das que realmente são eficazes. Diante dessa situação, não é incomum ver organizações optando por medidas de proteção de dados muito dispendiosas financeiramente, mas que não possuem a capacidade de oferecer o custo-benefício desejado. Para evitar desperdícios dessa natureza, recomenda-se a análise de riscos baseada nos seguintes objetivos:

Objetivo 1

Identificação dos ativos e seus valores: é calcado em ações de listagem dos principais ativos de uma organização e seus respectivos valores. Os ativos a serem listados podem ser primários, caracterizados por serem

indispensáveis ao funcionamento da organização. São representados por:

- A própria informação;
- Processos;
- Atividades relativas aos negócios da organização.

Há ainda os **ativos de suporte e infraestrutura**, os quais não são necessariamente obrigatórios para que uma organização seja bem-sucedida, mas oferecem importante apoio para que os ativos primários sejam estruturados e para facilitar as atividades de negócios de uma organização. São representados por:

- Hardware (computadores, laptops, impressoras, servidores, dentre outros);
- Software (de serviço, de manutenção, de administração, sistema operacional, dentre outros);
- Rede (switches, roteadores, cabos, dentre outros);
- Recursos humanos (decisores, usuários, pessoal de produção, de manutenção, de desenvolvimento);
- Instalações físicas (ambiente externo, edificações, áreas de acesso público e restrito, por exemplo);
- A própria estrutura da organização.

Objetivo 2

Determinação das ameaças e vulnerabilidades: as ameaças podem ser intencionais ou acidentais. Dependendo do contexto da organização, podem ser inúmeras, como:

- Danos físicos (causados por fogo, água, dentre outros);
- Eventos naturais (enchentes, seca e outros);
- Interrupção de serviços essenciais (luz, água etc.);
- Radiação eletromagnética e térmica;
- Espionagem;
- Escutas;
- Falhas técnicas;
- Ações não autorizadas;

- Hacktivismo;
- Pessoal interno insatisfeito.

As ameaças listadas abrangem uma grande parcela existente na atualidade, porém há várias outras ameaças que podem ser consideradas no processo de análise de riscos, de acordo com o contexto de cada organização. O fator de identificação de ameaça para uma organização reside na percepção de danos que possam advir de cada ameaça identificada. Em relação às vulnerabilidades, deve-se ter em mente que **qualquer ativo** pode apresentar uma vulnerabilidade, no entanto, sua presença não significa necessariamente que o risco será sempre concretizado, pois é necessário que a ameaça explore a vulnerabilidade identificada. Ainda assim, a identificação da vulnerabilidade deve ser considerada no processo de avaliação de riscos.

Objetivo 3

Determinação da possibilidade das ameaças tornarem-se reais: uma vez que as ameaças se concretizem, e interrompam os processos operacionais da organização, há um significativo impacto na organização.

Objetivo 4

Equilíbrio entre o custo do incidente e medida de segurança: objetivo caracterizado por avaliar os custos dos riscos à segurança da informação e das medidas para contê-los. Por exemplo, se uma empresa possui um servidor com dados avaliados em aproximadamente 50 mil reais, não valeria a pena medidas de segurança que custassem 100 mil reais. Muitas vezes, esse valor é altamente influenciado por exigências legais para a privacidade dos dados e até mesmo por danos a ativos imateriais, como a reputação e imagem de uma organização.

Exemplo

Se uma empresa possui um servidor com dados avaliados em aproximadamente 50 mil reais, não valeria a pena medidas de segurança que custassem 100 mil reais. Muitas vezes, esse valor é altamente influenciado por exigências legais para a privacidade dos dados e até mesmo por danos a ativos imateriais, como a reputação e imagem de uma organização.

Tais ativos são considerados altamente valiosos, pois a exposição negativa da imagem de uma empresa frente a incidentes envolvendo a informação de seus clientes, por exemplo, pode motivar a desistência por seus serviços, com eventuais prejuízos financeiros.

Pensemos na avaliação de riscos como uma forma de identificação, quantificação e priorização dos riscos para os quais a organização deverá dedicar tempo e dinheiro. Após efetuada a avaliação de riscos, haverá maiores chances de uma melhor implementação de controles

que realmente protejam os meios da Tecnologia da Informação de ameaças.

A avaliação de risco deve ser realizada periodicamente, devido à constante evolução dos requisitos de segurança, ameaças, ativos, vulnerabilidades e dos impactos à segurança dos dados, podendo ser realizada de forma quantitativa e qualitativa.

Tipos de análise do risco

Análise quantitativa

Esse tipo de análise visa ao cálculo de valores referentes ao prejuízo financeiro e à probabilidade de ameaças aos dados tornarem-se incidentes. Para calcular o valor do impacto de riscos nos negócios, deve-se identificar os custos de medidas de segurança, o valor de itens como hardwares, softwares, informações e diversos outros itens essenciais para o funcionamento da organização. Além disso, fatores como eventuais vulnerabilidades que podem ser exploradas, eficácia das medidas de segurança e intervalos prováveis de tempo em que um ameaça pode surgir devem ser levados em conta no valor calculado.

Atenção!

No processo de **análise quantitativa**, devem ser identificados os riscos aceitáveis, que são caracterizados por não possuírem medidas de segurança financeiramente viáveis, ou seja, o custo do bem a ser protegido e do risco relacionado são menores que o custo das medidas de segurança cabíveis.

Se utilizarmos apenas a análise quantitativa, poderemos obter uma noção do prejuízo financeiro decorrente do risco e quais medidas de segurança mais adequadas serão tomadas; no entanto, para exemplificarmos a dificuldade de cálculo do risco baseado apenas na análise quantitativa, tomemos como exemplo uma situação na qual uma organização possua vários servidores defeituosos. Podemos calcular aspectos como o valor de cada servidor novo ou com custo para sua manutenção, porém não é possível calcular com exatidão o valor dos dados armazenados em cada servidor. A informação contida nesses ativos possui valor variável, o qual será atribuído pela organização com critérios próprios, como o valor decorrente da perda ou indisponibilidade desses dados.

Análise qualitativa

A **análise qualitativa** não considera valores monetários para eventuais danos relacionados aos ativos cibernéticos de uma organização. Na verdade, o método qualitativo esboça situações com possibilidades de risco e classificação das ameaças de acordo com sua gravidade, bem como a validade da escolha de contramedidas específicas para contê-las. São exemplos de técnicas de análise qualitativa: aplicação de

melhores práticas conhecidas e experiência própria ou compartilhada, além da própria intuição e bom senso. Grupos de discussão, pesquisas, questionários, simulação de problemas, listas de verificação e reuniões são excelentes exemplos de técnicas qualitativas.

Uma análise qualitativa eficaz deve reunir um grupo de pessoas com experiência e conhecimento relacionado com as ameaças à organização da qual fazem parte. Esses profissionais qualificados devem realizar a proposição de um cenário que envolva prováveis ameaças, potenciais perdas, desdobramento de danos e, a partir desses elementos, mostrar as principais contramedidas por parte de todos que integram uma organização.

Exemplo

Em caso de corrompimento de dados, por exemplo, situação na qual é difícil atribuir com exatidão um valor monetário para a perda da integridade da informação, a análise qualitativa pode auxiliar na determinação, baseada nos critérios subjetivos apresentados, dos valores com métricas como “perda muito alta”, “perda muito baixa”, dentre outros tipos.

A seguir, vamos aprofundar o assunto em valoração dos ativos.

Valoração dos ativos

Como atribuir valor aos ativos

Ao identificarmos os **ativos informacionais** de fundamental importância para a organização, deveremos proceder com sua valoração, de forma que seja criada uma escala com o posicionamento do ativo e seu respectivo valor. Esse ativo poderá ter um valor quantitativo, sendo expresso por uma cifra na moeda local, ou, de forma qualitativa, poderá ser avaliado por termos como: valor insignificante, muito pequeno, pequeno, médio, alto, muito alto e crítico. O mesmo ativo pode ser valorado das duas formas, dependendo de como esse processo é conduzido por cada organização.

A atribuição de valor aos ativos é uma medida difícil, mas necessária no âmbito da segurança da informação e da segurança cibernética. Entre os diversos critérios de atribuição de valor, podemos utilizar o custo original e de substituição de um ativo, custos decorridos de ameaças à confidencialidade, integridade, disponibilidade, não repúdio, responsabilidade, autenticidade, confiabilidade dos ativos, bem como o valor da reputação de uma organização.

Os critérios a seguir podem auxiliar no processo de definição de um denominador comum para a valoração dos ativos:

- Violação da confidencialidade;
- Diminuição do desempenho do negócio;
- Violação de legislação ou regulamentação;

- Perda de valor de mercado;
- Efeito negativo sobre imagem e reputação;
- Violação de segurança de informações pessoais;
- Perigo ocasionado à segurança física das pessoas;
- Violação da ordem pública vigente;
- Perda financeira;
- Perigo ocasionado à segurança ambiental;
- Interrupção das atividades de negócio.

Lembrando que outros critérios poderão ser julgados pertinentes, de acordo com o contexto da organização.

Atenção!

A escala para definir o valor dos ativos poderá se confeccionada com níveis como muito baixo, baixo, alto e muito alto, dentre outros. No entanto, recomenda-se que esses níveis sejam estimados de acordo com critérios específicos para cada organização, pois, se uma organização define o valor dos ativos pelo seu custo nominal em moeda local, logicamente os menores custos serão classificados em níveis mais baixos e os maiores custos em níveis mais altos. Se for uma classificação puramente subjetiva, como o potencial dano por uma perda de dados importantes, não será apropriada uma nivelação em valores financeiros, mas sim em mais valiosos ou menos valiosos para aquela organização.

No processo de valoração de ativos, também se considera a dependência que processos relativos aos negócios possuem em um ativo. Quanto maior o número e a relevância dos processos associados ao ativo, maior o valor dele.

Exemplo

Se um ativo, como uma sala de servidores, depende do resfriamento de um ar-condicionado para que não seja danificado e evite o comprometimento da integridade dos dados ali guardados, os custos relacionados ao ar-condicionado deverão ser contabilizados no valor atribuído à integridade dos dados. Da mesma maneira, se a sala de uma empresa possui controle biométrico para acesso apenas de pessoas autorizadas, deverão ser contabilizados os custos relacionados ao hardware e software utilizados por esse controle no valor final atribuído à confidencialidade dos dados que residem na sala.

Para facilitar o processo de valoração de ativos dependentes, é importante verificar as seguintes situações:

Valores menores ou iguais

Caso os valores de ativos dependentes, como os dados, sejam menores ou iguais ao valor do ativo em questão, como o computador, o valor do último permanece o mesmo.

Valores maiores

Caso os valores dos ativos dependentes sejam maiores que do ativo em questão, é recomendável que o valor desse último se eleve de acordo com o grau de dependência ou valores dos outros ativos.

A etapa de valoração dos ativos será considerada concluída quando puder elencar a lista de todos os ativos da organização, bem como seus respectivos valores relativos à divulgação imprópria e/ou ilegal de informações, a modificações não consentidas, à indisponibilidade e destruição do ativo e ao custo de sua reposição.

Percebe-se que esse processo de atribuição de valores aos ativos do meio cibernético está intimamente ligado a potenciais danos ao acrônimo CID (confidencialidade, integridade e disponibilidade) e demais propriedades da Segurança da Informação.

Avaliação do impacto do risco

Critérios para avaliação

Após a etapa de **valoração**, faz-se necessária uma avaliação do impacto do risco aos ativos da organização. O nível do impacto está diretamente relacionado ao sucesso de a ameaça causar algum dano, em maior ou menor grau, para os ativos. Nesse sentido, cabe destacar que o mesmo incidente poderia causar diferentes níveis de danos a diferentes organizações, dependendo do nível de maturidade de proteção de dados, bem como do tipo de impacto, o qual pode ter efeito imediato (operacional) ou futuro (relativo aos negócios da organização como um todo). Tais efeitos estão intrinsecamente associados aos aspectos financeiros e de mercado.

O **impacto imediato** pode ser direto ou indireto. O direto é aferido de acordo com:

- Valor financeiro de substituição do ativo perdido ou de parte dele;
- Custo de aquisição, instalação e configuração do ativo reposto ou de backup;
- Custo das transações de negócios suspensas devido à ocorrência de incidentes, o qual cessa após o restabelecimento do ativo ou ativos que gerenciam as transações.

Já o **impacto indireto** é dado por fatores como:

- Custo de oportunidade, ou seja, o custo de alocar recursos financeiros em reparos de ativos ao invés de aplicar tais recursos em outro fim benéfico para a

organização, como aquisição de novos ativos;

• Mau uso de informações coletadas por violações de segurança;

• Violação de obrigações descritas em normas ou estatutos regulatórios;

• Violação de códigos éticos.

O valor do cálculo financeiro resultante da estimativa do impacto de riscos será muito maior sem a implementação de controles de segurança eficazes que protejam os ativos de uma organização, porém tal valor poderá diminuir consideravelmente após tais controles serem adotados é dado por fatores como:

Estimativa do impacto financeiro associado a ameaças

Existem **fórmulas** que auxiliam na determinação de valores monetários referentes à probabilidade de danos em decorrência de ameaças. É possível calcular potenciais perdas monetárias utilizando-se de dados como valores de ativos e probabilidades de ocorrências de incidentes com as seguintes fórmulas:

EF (*exposure factor*)

Fator de exposição. Representa a estimativa, em porcentagem, da perda provocada por uma ameaça em um ativo. Por exemplo, uma empresa que anualmente fatura com vendas pela internet pode estimar que haja uma EF de valor igual a 0,27% em caso de incidente cibernético ao seu site de vendas que o deixe indisponível por um dia. Tal valor foi obtido mediante o cálculo percentual de lucro diário, dividindo-se 100% por 365 dias do ano. Obviamente, outros tipos de critérios também podem ser utilizados para obter a EF.

SLE (*single loss expectancy*)

Expectativa de perda singular, calculada com base em apenas um evento, representando a potencial perda da organização caso uma ameaça específica ocorra. Para calcularmos a SLE, devemos mensurar o valor do ativo e da EF. SLE = valor do ativo x EF. No caso anterior, o site de vendas da empresa possuía um valor de R$ 500.000,00 em faturamento anual e a EF era de 0,27%. Como o valor de 500.000,00 representa 100% do valor, nesse caso 0,27% representaria uma SLE diária de R$ 1.350,00.

ARO (*annualized rate of occurrence*)

Taxa de ocorrência anual. Representa uma estimativa da frequência de ocorrências de ameaças específicas no período de 1 (um) ano. Seu valor não pode ser menor que 0 (zero), pois isso significa que a ameaça nunca ocorrerá. Se for 1 (um), a ameaça pode ocorrer pelo menos uma

vez ao ano. Para obter seu valor, basta dividir o número de vezes que a ameaça pode ocorrer pelo período de tempo definido por anos. Supondo que a empresa tenha probabilidade de sofrer 10 (dez) ataques cibernéticos por ano, sua ARO é obtida dividindo-se 10 por 1, ou seja, uma ARO de valor 10.

ALE (*annualized loss expectancy*)

Expectativa de perda anual representada pela seguinte fórmula: ALE = SLE x ARO. No exemplo anterior, a ALE seria de R$1.350,00 x 10, o que daria um prejuízo anual esperado no valor de R$13.500,00. Partindo-se do princípio de que esse cálculo foi feito pela empresa sem levar em consideração as medidas de cibersegurança, podemos dizer que, se tais medidas forem adotadas, haverá uma diminuição considerável nessa estimativa de prejuízo.

Gerenciamento de riscos em segurança da informação

Veja a seguir uma abordagem dos principais aspectos e requisitos do processo de gerenciamento de riscos na proteção de dados de uma organização.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Especialistas em segurança cibernética de uma empresa receberam a tarefa de listarem todos os seus ativos pertencentes ao meio cibernético e seus respectivos valores. O intuito era fornecer subsídios adequados para as decisões sobre os tipos de controles de segurança que seriam aplicados para a segurança cibernética de uma empresa. Com isso, assinale a alternativa que apresenta o ativo e seu respectivo tipo.

A

Celulares (ativo de suporte e infraestrutura), computadores (ativo de suporte e infraestrutura) e as informações neles contidas (ativo de suporte e infraestrutura).

B

Software de manutenção (ativo de suporte e infraestrutura), sistema operacional proprietário (ativo primário) e as informações inseridas nesses ativos (ativo primário).

C

Software de manutenção de ativos (ativo de suporte e infraestrutura), software de transações de negócios (ativo de suporte e infraestrutura) e as atividades de negócios da empresa (ativo primário).

D

Recursos humanos (ativo primário), software de administração da Folha de Pagamento (ativo de suporte e infraestrutura) e os processos gerenciais da empresa (ativo de suporte e infraestrutura).

E

Impressoras (ativo de suporte e infraestrutura), laptops (ativo de suporte e infraestrutura) e roteadores (ativo primário).

Parabéns! A alternativa C está correta.

O tipo de ativo identificado no processo de análise de riscos envolve duas classificações: ativos primários e ativos de suporte e infraestrutura. O primeiro tipo envolve a informação, os processos e as atividades de negócios de uma organização, ou seja, são ativos criados pela própria empresa. Quanto aos ativos de suporte e infraestrutura, sua principal característica é apoiar a inserção dos ativos primários em sua estrutura, podendo ser incluídos itens como softwares de manutenção e transações, os quais fazem o apoio para gerenciamento de informações de uma organização.

Questão 2

Uma empresa sofre com o risco de incêndio em sua sala de servidores e de armazenamento de informações sensíveis, utilizada para abrigar informações de usuários, bem como o próprio site de vendas do produto. Estima-se que, depois de um incidente dessa natureza, pode-se ter um dano físico ao percentual de 20% de todo o hardware, bem como a impossibilidade de funcionamento do site por vários dias e perda de informações de clientes. Assinale a

alternativa que indica **apenas** critérios corretos para avaliação do impacto financeiro, baseando-se no risco de incêndio.

A	Custo de oportunidade para reparo do material da sala e violações de códigos éticos referente às informações dos funcionários e clientes.
B	Mau uso de informações coletadas dos funcionários e clientes e custo de aquisição de material novo.
C	Custo de aquisição de material novo e violações de leis de privacidade dos dados.
D	Violação de códigos éticos e violação de leis de proteção aos dados.
E	Custo das transações de venda do produto perdidas, devido à interrupção do funcionamento do site, e o custo com backup das informações dos clientes.

Parabéns! A alternativa E está correta.

Referente à perda de informações e do hardware contido na sala dos servidores e de armazenamento de informações, deveriam ser associados critérios de impactos referentes ao valor de reposição dos itens perdidos, em caso de incêndio. Não haveria prejuízo às leis ou a aspectos éticos em decorrência de um incêndio na sala, pois o incêndio poderia acarretar apenas uma perda da disponibilidade e não da confidencialidade dos dados. Além disso, devido à interrupção do funcionamento do site de vendas, o valor do lucro que normalmente seria adquirido em decorrência de vendas deveria ser considerado no valor do impacto financeiro.

4 - Plano de cibersegurança (*Cybersecurity Plan*)

Ao final deste módulo, você será capaz de identificar os aspectos necessários para a criação do plano de cibersegurança (*Cybersecurity Plan*).

Mitigação do risco

Estratégias

Dentro do contexto do **gerenciamento de risco**, após avaliarmos os valores dos ativos e o impacto das ameaças, devemos agora elaborar uma estratégia com o objetivo de tratarmos o risco da maneira mais adequada para a organização. Por isso, há três tipos de estratégias mais comuns para lidarmos com o risco:

1. Prevenção ou anulação do risco.
2. Tolerância ao risco.
3. Redução ou minimização do risco.

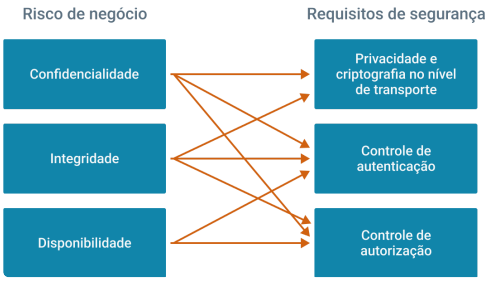
A **prevenção do risco** visa neutralizar a ameaça e impedir um incidente. Um exemplo seriam atualizações em banco de dados de antivírus, ou

seja, é uma ação de caráter preventivo que impede que novos tipos de malwares possam infectar os ativos de TI.

A **redução do risco** objetiva aplicar medidas que impeçam a ameaça de causar um incidente e, se o fizer, tenta-se diminuir o resultado do dano. Podemos exemplificar a redução do risco quando os funcionários de uma empresa são orientados a não abrirem e-mails de origem duvidosa, pois alguns podem estar infectados com malwares, por exemplo. Em virtude da orientação, a maioria dos funcionários não abrirá esse tipo de e-mail, no entanto, por descuido, alguns poderão abrir e infectar seus computadores de trabalho. De toda forma, o impacto será muito menor em virtude da quantidade pequena de funcionários que abrirem o e-mail infectado.

A **tolerância ao risco** é a estratégia que permite a aceitação dos danos provenientes das ameaças, pois muitas vezes o eventual prejuízo é menor que os custos de controles de segurança a serem adotados para anulá-lo. Dessa forma, a organização poderá escolher pela opção de aceitar o risco.

Como exemplo de mapeamento de riscos nas atividades de negócios de uma organização, a imagem a seguir traz alguns requisitos de segurança que poderão atuar de forma a minimizá-los ou anulá-los. Cada propriedade da segurança cibernética poderá ser preservada de acordo com os seguintes requisitos:



Exemplo de mapeamento de riscos e requisitos de segurança.

Tratamento do risco

Após uma triagem da organização sobre a avaliação geral dos riscos aos quais estará sujeita e, dentre os riscos avaliados, quais serão aceitos, reduzidos ou mitigados, procede-se ao **planejamento das medidas de tratamento dos riscos**. Tais medidas poderão caracterizar-se por:

Aplicar os devidos controles de segurança para redução dos riscos.

Aceitar racional e objetivamente os riscos.

Evitar que o risco se torne incidente.

Transferir o risco a terceiros, como fornecedores ou seguradoras, caso haja responsabilidade desses entes.

Implementar, se houver, controles definidos para lidar com o risco, de acordo com o estritamente idealizado durante a fase de avaliação de riscos.

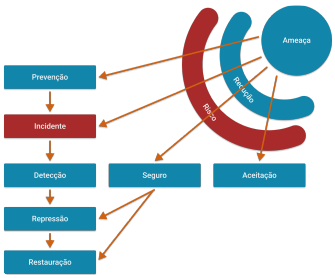
Especificamente em relação à **estratégia de redução do risco**, deve-se implementá-la de acordo com os seguintes aspectos:

- Objetivos da organização;
- Normas da legislação e eventuais regulamentos nacionais ou internacionais;
- Restrições e requisitos das operações da organização;
- Equilíbrio de investimento entre o custo de mitigar o risco e o dano causado;
- Custo de adoção e operacionalização da medida de tratamento de risco proporcional às limitações e exigências da organização.

Dentro do contexto de segurança da informação de cada organização, os controles escolhidos para redução de riscos poderão ser bem-sucedidos, mas há de se entender que não há segurança integralmente plena. Diante disso, são necessárias ações como monitoramento, avaliação e melhoramentos quanto à eficiência e eficácia dos controles de segurança.

Contramedidas para mitigação do risco

Uma análise de riscos bem-estruturada pode oferecer a quantidade e a relevância de ameaças a uma organização. Dessa forma, podem ser propostas contramedidas para minimizar as consequências e/ou reduzir as chances de ocorrência de um incidente. As **contramedidas de segurança** podem ser ilustradas na imagem a seguir.



Contramedidas de mitigação do risco.

Podemos caracterizar as contramedidas ilustradas na imagem anterior da seguinte forma:

Contramedidas de prevenção

São as que objetivam evitar os incidentes.

Exemplo: instalação de firewall para inibir conexões de rede ilegítimas e credenciamento de funcionários para evitar acesso não autorizado a locais restritos.

Contramedidas de redução

São as que visam diminuir a probabilidade de uma ameaça se concretizar.

Exemplo: utilização de classificação das informações sensíveis de uma organização com o intuito de diminuir o número de pessoas que possam ter acesso a essas informações.

Contramedidas de detecção

São aquelas que fornecem um alerta a ameaças e ajudam a minimizar um possível dano.

Exemplo: utilização de ferramentas capazes de detectar uma navegação imprópria de funcionários em sites da Internet.

Contramedidas de repressão

São as que ocorrem quando há evidências de que uma atividade irregular ocorreu e pode trazer algum tipo de dano, ações repressivas podem combater a ameaça e diminuir os danos.

Exemplo: medidas de segurança para apagar um incêndio e interrupção do tráfego de Internet após a identificação de um incidente.

Contramedidas de restauração

São as utilizadas para recuperação de eventuais danos causados.

Exemplo: utilização de backups para recuperação de arquivo.

Aceitação do risco

Ocorre quando nenhuma medida de segurança é adotada para mitigar os riscos.

Exemplo: se um empregado vai ser demitido por má desempenho, há a possibilidade que ele entre na justiça contra a empresa, que pode aceitar esse risco e não fazer nada a respeito, já que se trata de um direito do ex-funcionário.

Uso de seguro para transferência do risco

É a ação pela qual propõe-se aliviar consequências de eventos que não possam ser totalmente prevenidos, mas que representam danos custosos.

Exemplo: acionar o seguro por perda total das informações de uma organização em decorrência de fenômenos da natureza como descargas elétricas, enchentes, dentre outros.

Conceituação do plano de cibersegurança

Características do plano

O **plano de cibersegurança** é um documento que prevê as principais medidas de segurança para proteção dos ativos cibernéticos de interesse de uma organização. O desenvolvimento e execução desse plano não sofrem com atualizações da tecnologia dos ativos, pois sua estruturação não é composta de medidas específicas para cada tipo de ativo, mas sim de padronizações e melhores práticas reconhecidas mundialmente.

O objetivo do plano de cibersegurança é minimizar o desperdício de recursos de uma organização ao gerenciar os riscos para segurança cibernética. Além disso, o plano é importante para evitar ao máximo a ocorrência de eventuais danos causados por incidentes cibernéticos.

> **Não há um modelo único de plano de cibersegurança que possa ser utilizado de forma geral, pois cada organização poderá mapear riscos, ameaças e vulnerabilidades de forma diferente.**

As ações diretoras para a **fundamentação do plano de cibersegurança** são:

• Descrever a situação atual das medidas utilizadas no contexto da segurança cibernética;

• Descrever o estado ideal de implementação da segurança cibernética;

• Identificar e priorizar oportunidades para o constante aperfeiçoamento das medidas de segurança cibernética, face a novas ou antigas ameaças;

• Assessorar quanto à maturidade de segurança cibernética alcançada;

• Comunicar-se com entes internos e externos interessados sobre os riscos para segurança cibernética da organização.

O plano de cibersegurança deverá ser documentado e sempre atualizado, em virtude da manifestação e evolução de antigas, atuais e novas ameaças do meio cibernético. Por essa razão, a organização deverá desenvolver formas de atualizar constantemente seu plano de cibersegurança. Para essa tarefa, poderá valer-se do modelo **PDCA** (*Plan-Do-Check-Act*), ou em português, Planejar-Executar-Checar-Agir. O modelo PDCA pode ser descrito da seguinte forma:

Planejar

Nesta fase, a finalidade é desenvolver e documentar a política de segurança cibernética, demonstrando como os objetivos a serem alcançados com as medidas de segurança, baseadas na análise de riscos e custo-benefício, podem auxiliar os objetivos de negócios da organização.

Executar

Nesta fase, todo o planejamento documentado para a política de Segurança Cibernética será executado.

Checar

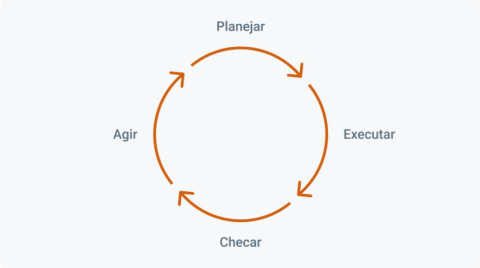
Esta fase busca realizar controles de auditoria interna com o intuito de monitorar se as ações previstas para a política de Segurança Cibernética estão sendo executadas, conforme planejamento.

Agir

Esta fase final tem o objetivo de realizar correções para retroalimentar o ciclo do PDCA, ou seja, ao serem observados os resultados do planejamento inicial, podem ser propostas

melhorias ou correções, durante a fase de “Planejar”, das medidas de segurança previstas no Plano de Cibersegurança.

Veja, na imagem a seguir, o desenho do modelo PDCA.



Representação do ciclo PDCA.

Com o ciclo PDCA disposto na imagem anterior, dispomos de uma forma dinâmica e ampla para criarmos, executarmos, monitorarmos e melhorarmos o plano de cibersegurança.

Fases do plano de cibersegurança.

A **estruturação do plano de cibersegurança**, conforme a imagem anterior, pode ser dividida em cinco fases:

Identificação

É a fase com foco na enumeração dos riscos de ameaças cibernéticas a sistemas, dados, capacidades, recursos humanos e demais ativos de uma organização. Identificar é o primeiro passo para entender o contexto de negócios, os riscos e os recursos que alimentam processos críticos de uma organização. Dessa forma, poderá ser feita a priorização de esforços consistentes com a estratégia de negócios e gerenciamento dos riscos.

Proteção

É a fase com a tarefa de desenvolvimento e adoção de contramedidas de segurança para garantia do funcionamento dos processos regulares e críticos de uma organização. Com essa ação, busca-se a minimização ou contenção do impacto de um incidente cibernético.

Detecção

É a fase responsável por implementar atividades necessárias para detecção de um incidente cibernético. Essa ação objetiva a catalogação de incidentes cibernéticos agrupados em uma linha temporal, permitindo a visualização do momento em que ocorreram.

Resposta

É a fase que permite desenvolver e adotar atividades para lidar com os incidentes cibernéticos detectados.

Recuperação

É a fase que induz ao desenvolvimento e à implementação de atividades importantes para manter a resiliência e recuperação de ativos impactados por um incidente cibernético.

Estruturação do plano de cibersegurança

Fases do plano

As fases definidas pelas ações de identificação, proteção, detecção, resposta e recuperação possuem várias medidas importantes para serem aplicadas no contexto da atividade de segurança cibernética. Essas medidas funcionam como um checklist, ou seja, são atividades desempenhadas em cada fase do processo de estruturação do plano de cibersegurança. Veja a seguir.

Identificação

Podemos definir a fase da identificação pelas seguintes medidas:

- Listagem dos principais ativos para a organização, como hardware, sistemas de informação internos e externos, softwares, aplicações, fluxograma de dados, comunicações da organização, recursos humanos e tempo. Cada um desses ativos deverá constar em uma ordem de prioridade baseada em características como valor, criticidade e classificação;

• Listagem das responsabilidades pela segurança cibernética de todos os funcionários e para terceiros, como acionistas, fornecedores, clientes e parceiros;

• Verificação de prioridades de missões, objetivos, dependências de outras organizações, sistemas e funções críticas e atividades de negócios para a organização;

• Verificação da importância da organização para o setor de negócios em que se insere;

• Estabelecimento de critérios para medir a resiliência dos serviços críticos da organização, seja em ambiente de normalidade, incidente cibernético ou recuperação de incidentes;

• Estabelecimento da governança cibernética da organização respaldada em regulações e normas jurídicas, as quais incluem privacidade, garantias e direitos individuais;

• Compartilhamento de informações sobre ameaças cibernéticas em fóruns colaborativos e a partir de fontes seguras;

• Avaliação do impacto do risco para os negócios com a listagem de ameaças internas e externas, vulnerabilidades e probabilidades de incidentes. Além disso, a organização deverá enumerar os riscos a serem tolerados ou mitigados, além de identificar os indivíduos responsáveis pelo gerenciamento de riscos, sejam eles funcionários da organização ou terceiros, respeitando o que for acordado em contrato com esses entes;

• Identificação e priorização de responsabilidades pelo gerenciamento de riscos.

Proteção

Podemos definir a fase da proteção pelas seguintes medidas:

• Checagem da execução correta de emissão, gerenciamento, verificação e revogação de identidades e credenciais dos indivíduos vinculados à organização;

• Auditoria de dispositivos autorizados, usuários e processos;

• Proteção e gerenciamento de acesso físico aos ativos, quando for o caso;

• Gerenciamento de acesso remoto aos ativos;

• Gerenciamento de permissões de acesso e autorizações baseadas no princípio da segregação de funções, ou seja, aplicar a categorização das informações somente para os grupos ou indivíduos que realmente necessitem ter acesso;

• Proteção da integridade da rede com uso de segregação e segmentação de redes, por exemplo;

• Uso de autenticação simples ou complexas de usuários, dispositivos e outros ativos de acordo com o impacto de risco vinculado ao ativo, sendo que ativos mais importantes deverão possuir autenticações mais complexas, decaindo o grau de complexidade de acordo com a importância do ativo;

• Conscientização e treinamento de todos os usuários, diretores, clientes, fornecedores e parceiros com relação às medidas de Segurança Cibernética, bem como as responsabilidades e funções de cada um, principalmente dos usuários com mais privilégios de acesso;

• Proteção para dados armazenados e enviados;

• Notificação formal dos ativos que forem removidos, transferidos e dispostos;

• Viabilização de capacidade adequada que permita a disponibilidade da informação;

• Aplicação de medidas de proteção contra vazamento de dados;

• Aplicação medidas de checagem da integridade de softwares, hardwares, firmwares e da informação;

• Separação do ambiente de desenvolvimento e teste do ambiente de produção;

• Criação e manutenção de uma configuração básica para os sistemas de controle da Tecnologia da Informação com base em princípios da Segurança Cibernética;

• Desenvolvimento de um sistema para gerenciamento do ciclo de vida dos sistemas da organização;

• Início, manutenção e teste de backups de informações;

• Destruição de dados de acordo com a política da organização;

• Compartilhamento da constatação da efetividade de medidas de proteção;

• Criação e gerenciamento dos planos de Resposta a

Incidentes, Continuidade de Negócios, Recuperação de Incidentes e Desastres;

• Criação e implementação de um plano de gerenciamento de vulnerabilidades;

• Aprovação e verificação das atividades de reparo e manutenção em ativos. Isso também vale para ações de forma remota, com o intuito de prevenir acessos não autorizados;

• Gravação, documentação e implementação de logs de auditoria, conforme a política da organização;

• Estabelecimento do uso restrito e seguro de mídias removíveis;

• Proteção às redes de comunicação e controle.

Detecção

Podemos definir a fase da Detecção pelas seguintes medidas:

• Identificação e gerenciamento da situação esperada para o comportamento normal do fluxo de dados e dos processos executados em rede nos sistemas utilizados, o que facilita a detecção de eventos anômalos para a organização;

• Detecção e análise de eventos anômalos para tentar entender os alvos e métodos das ameaças;

• Coleta e correlação dos dados de eventos com os sensores e diversas outras fontes;

• Determinação do impacto dos eventos;

• Estabelecimento de mecanismos de alertas em diferentes níveis, de acordo com o impacto da ameaça;

• Monitoramento da rede e do ambiente físico com o intuito de detectar potenciais eventos relativos a incidentes cibernéticos;

• Monitoramento das atividades relativas aos integrantes da organização com o objetivo de detectar potenciais incidentes cibernéticos;

• Implantação de mecanismos para a detecção de código malicioso;

• Monitoramento de acesso não autorizado de pessoas, dispositivos, conexões e softwares;

• Realização de escaneamento de vulnerabilidades;

• Definição das funções e responsabilidades de todos os envolvidos no processo de detecção de ameaças;

• Testagem prévia de processos de detecção;

• Reporte e aperfeiçoamento constante da detecção de eventos e ameaças cibernéticas;

Resposta

Podemos definir a fase da “Resposta” pelas seguintes medidas:

• Encadeamento das medidas dessa fase em um plano de resposta a incidentes e execução durante ou após o incidente cibernético;

• Conscientização do pessoal envolvido na Segurança Cibernética acerca da sua função e da ordem das atividades a serem executadas quando for necessária a resposta a incidentes cibernéticos;

• Comunicação dos incidentes de forma consistente com o critério adotado para essa atividade;

• Adoção de coordenações com organizações parceiras, dentro da necessidade e do contexto, com o intuito de aplicar as medidas planejadas para o plano de resposta à incidentes cibernéticos;

• Compartilhamento, voluntário, de informações sobre ameaças cibernéticas com outras organizações;

• Investigação de notificações sobre as detecções de eventos anômalos;

• Avaliação do impacto dos incidentes cibernéticos;

• Aplicação da atividade de Forense Digital, quando for o caso, para entender-se a origem e as consequências dos incidentes cibernéticos;

• Categorização dos incidentes cibernéticos;

• Estabelecimento de processos para receber, analisar e responder a vulnerabilidades descobertas. Essas

vulnerabilidades devem ser mitigadas ou classificadas como riscos aceitáveis;

• Contenção e mitigação dos incidentes;

• Inserção de lições aprendidas com incidentes prévios no processo de atualização do plano de respostas a incidentes.

Recuperação

Podemos definir a fase da “Recuperação” pelas seguintes medidas:

• Encadeamento das medidas dessa fase em um plano de recuperação a incidentes e execução durante ou após o incidente cibernético;

• Inserção das lições aprendidas com incidentes prévios no plano de recuperação;

• Atualização constante das estratégias de recuperação dos ativos;

• Gerenciamento das atividades de relações públicas condizentes com o intuito de diminuir o impacto negativo à reputação após um incidente cibernético;

• Comunicação das atividades de recuperação dos ativos e das informações a todos os entes interessados, sejam eles integrantes da organização ou terceiros.

Criando o plano de cibersegurança

Veja a seguir uma abordagem das principais características do plano de cibersegurança segundo ‘NIST Cybersecurity Framework’.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Marcos, especialista em segurança cibernética, verificou em sua organização que havia uma série de medidas a serem tomadas para impedir que incidentes cibernéticos não ocorressem. Essas medidas podem ser enquadradas em qual categoria de contramedidas para mitigação do risco?

A Contramedidas de prevenção.

B Contramedidas de repressão.

C Contramedidas de redução.

D Contramedidas de restauração.

E Contramedidas de detecção.

Parabéns! A alternativa A está correta.

As contramedidas de prevenção são as mais indicadas para evitar um incidente cibernético.

Questão 2

Durante a estruturação do Plano de Cibersegurança de sua organização, Carla observou que havia a necessidade de medidas eficazes após a detecção de atividades anômalas que poderiam fazer parte de um possível incidente cibernético. Diante disso, qual a fase caracterizada pelos eventos de criação e implementação de medidas que façam frente aos incidentes cibernéticos detectados?

A Identificação

B Recuperação

C Detecção

D Resposta

E Proteção

Parabéns! A alternativa D está correta.

Após a detecção de incidentes cibernéticos, a fase seguinte, a da Resposta, é responsável por permitir que sejam adotadas medidas responsivas para lidar com os incidentes cibernéticos detectados.

Considerações finais

Vimos, ao longo deste conteúdo, vários acontecimentos relacionados a ameaças cibernéticas, os quais foram responsáveis pela progressiva evolução das medidas de Cibersegurança, desde o século passado.

Visualizamos também que não só o capital e os meios de produção possibilitam o sucesso nas atividades de negócios, mas também o modo como se atribui valor e proteção às informações que fazem parte dos ativos de uma organização. Tal proteção necessita de recursos financeiros, os quais são proporcionais ao risco envolvido no contexto cada ativo.

Por fim, consolidamos todos os conhecimentos apresentados referentes à segurança da informação e à segurança cibernética para fundamentação do plano de cibersegurança, o qual é responsável por anular ou mitigar os incidentes cibernéticos, com o objetivo de reduzir prejuízos de qualquer natureza para uma organização.

Podcast

Ouça agora um resumo dos principais assuntos abordados até aqui.

Para ouvir o *áudio*, acesse a versão online deste conteúdo.

Explore +

Assista ao filme **Snowden – Herói ou Traidor** (2016), longa-metragem que traz aspectos interessantes sobre a quebra da confidencialidade de dados sensíveis para o Governo dos Estados Unidos da América.

Leia o livro **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**, de Richard A. Clarke e Robert K. Knake, o qual revela o papel da guerra cibernética como modeladora do contexto geopolítico atual.

Leia o modelo de estruturação do **Plano de Segurança da Informação, Comunicações e Segurança Cibernética**, desenvolvido pelo governo brasileiro, para verificar a execução dos princípios e conceitos de Segurança Cibernética abordados neste conteúdo.

Referências

ABNT. **NBR ISO/IEC 27005:2011** – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2011.

AO KASPERSKY LAB. **O que é uma ameaça persistente avançada (APT)?** [s. d.] Consultado na internet em: 17 jan. 2022.

CRONIN, B. **Esquemas conceituais e estratégicos para a gerência da informação**. Revista da Escola de Biblioteconomia da UFMG, Belo Horizonte, 1990. Consultado na internet em: 20 dez. 2021.

AMARAL, L. A. M. **Praxis**: Um Referencial Para O Planeamento De Sistemas De Informação. 1994. Tese de Doutorado. Universidade do Minho (Portugal).

FOVINO, I. N. *et al*. **Cybersecurity, our digital anchor**. *In*: BARRY, G.; DEWAR, M.; MORTARA, B. (ed.). Luxemburgo: Publications Office of the European Union, 2020. Consultado na internet em: 15 dez. 2021.

KLIMBURG, A. **National Cyber Security Framework Manual**. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012. Consultado na internet em: 15 dez. 2021.

MARVIN THE ROBOT. **Stuxnet**: As origens. Kaspersky Lab, 20 nov. 2014. Consultado na internet em: 17 jan. 2022.

NIST. National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity**. 2018. Consultado na internet em: 5 jan. 2022.

PORTELA, L. S. **Geopolítica do espaço cibernético e o poder**: o exercício da soberania por meio do controle. Revista Brasileira de Estudos de Defesa, [s. l.], v. 5, n. 1, p. 141-165, jan./jun. 2018. Consultado na internet em: 17 jan. 2022.

SMULDERS, A. *et al*. **Fundamentos de Segurança da Informação**: Com base na ISO 27001 e na ISO 27002. Tradução: Alan De Sá. 3. ed. rev. Rio de Janeiro: BRASPORT Livros e Multimídia, 2018.

Material para download

Clique no botão abaixo para fazer o download do conteúdo completo em formato PDF.

Download material

O que você achou do conteúdo?

Relatar problema