PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO 1 – CONCEITOS E DEFINIÇÕES DA SEGURANÇA DA INFORMAÇÃO E SEUS PRINCÍPIOS

Dr. Halley Wesley Alexandre Silva Gondim

Introdução

Hoje, é praticamente impossível, ou incomum, encontrar pessoas que nunca acessaram a *Internet* por meio direto, através de um dispositivo pessoal como o *celular*, o *tablet*, o *computador* ao acessar as diversas redes sociais, *sites* etc., ou de forma indireta ao interagir com um terminal de um caixa eletrônico, por exemplo. Sem dúvida, a *Internet* conseguiu conectar o mundo, trazendo qualquer informação instantaneamente aos nossos olhos. Em consequência disso, uma nova era começou, a era da informação (SÊMOLA, 2014).

Com toda essa conectividade e conhecimento houve também o surgimento de diversos inconvenientes. A informação que trafegava sem problemas agora passou a ser espionada, dados antes tidos como seguros passaram a ser inseguros. Ataques contra a privacidade, espionagem, desvio etc. passaram a ser assuntos bastante comuns. Em meio a esse caos, houve a necessidade de proteger a informação e logo surgiu a Segurança da Informação.

Tal área é responsável por garantir a segurança dos dados e para que isso ocorra é necessária uma série de ações e medidas oriundas de padrões definidos internacionalmente. Tais padrões servirão de norte para políticas de manipulação das informações as quais serão vistas neste capítulo.

Ao nos referenciarmos sobre a Segurança da Informação, você toma algum cuidado com a manipulação de seus dados pessoais? Seus dados estão na *Internet* de forma segura? Você já foi enganado por falsos contatos de empresas (*e-mail*, telefone, *SMS* etc.)? Você sabia que existem normas internacionais para garantir a segurança de seus dados? É sobre essas questões que trataremos aqui.

1.1 O que é informação?

Desde os primórdios da humanidade houve a necessidade de se comunicar por meio de desenhos, de gestos, de sinais, de sons e tais elementos tinham o objetivo de indicar alguma informação ou até mesmo perpetuar um conhecimento importante para gerações posteriores. Atualmente, não é diferente, porém, a quantidade de dados produzida é exponencial a cada ano. Logo, é essencial que ocorra um gerenciamento de tais dados e que eles estejam devidamente seguros de acordo com o grau de sua importância.

Em decorrência dessa explosão de dados surgiram diversas áreas como a Segurança da Informação, a Recuperação da Informação (há dados, mas como recuperá-los?), a Visualização de Informações (visualizar uma coleção enorme de dados por meio visuais auxilia na tomada de decisão), a *Big Data* (área responsável por gerir enormes quantidades de dados e obter informações não triviais) entre outras (SÊMOLA, 2014). Como o foco de nosso estudo é a Segurança da Informação começaremos do básico até adentrar cada vez mais nessa área.

No parágrafo anterior apareceram alguns termos relacionados à comunicação, dentre os quais podemos destacar “dado”, “informação” e “conhecimento”. Entretanto, ao tentar defini-los, a princípio, é possível que se gere certa confusão. Então, a seguir, descreveremos cada um deles indicando a hierarquia entre si, juntamente com o conceito de “comunicação”. Tais definições irão nos ajudar a compreender os termos nas próximas seções.

Figura 1 - Analisando informações.
Fonte: Shutterstock, 2019. http://mediapool.fabrico.com.br/index.php/tagueadas-02/iStock-957654606

Ao nos referirmos o termo “dado”, indicamos que ele está sendo armazenado de alguma forma, porém, não há nenhum sentido para um ser humano e nem para um computador uma vez que o dado é apenas uma sequência de *bits* sem nenhum contexto (HINTZBERGEN *et al.*, 2018). É bem provável que para você, por exemplo, o dado 34435 não tenha nenhum sentido e não lhe seja útil.

Por outro lado, a “informação” é a contextualização de um dado, ou seja, é quando um conjunto de dados passa a ter sentido (HINTZBERGEN *et al.*, 2018). Por exemplo, imagine que você tenha recebido uma lista com 50 números com 11 dígitos cada. *A priori*, a lista não tem nenhuma lógica, mas depois de alguns minutos a pessoa que lhe entregou a lista lhe informa que a lista tem o título que ela havia se esquecido de colocar ao lhe entregar: “Relação de aprovados no vestibular por número de CPF”. Antes, você tinha um dado sem sentido, agora você tem uma informação relativa às pessoas aprovadas em um vestibular.

Em último nível temos o termo “conhecimento”. Ele está diretamente relacionado com diversas informações interconectadas de forma lógica. Em nosso exemplo anterior, podemos dizer que aquela lista de aprovados do vestibular é dos candidatos do Curso de Direito que obtiveram as melhores notas nos últimos dois anos. Observe que com um conjunto de informações conseguimos obter respostas mais elaboradas, pois cruzamos diversas informações para obter algo maior.

Tendo em mente esse conceito, nos deparamos com um grande problema, ou seja, a quantidade de dados, sua variedade e a velocidade com que crescem é sem dúvida um dos grandes desafios para a TI (Tecnologia da Informação). A EMC Corporation (hoje, DellEMC, uma empresa de armazenamento e segurança de dados) estimou que em 2020 haja 44 *zettabytes* gerados no mundo. Imagine a complexidade que é gerenciar e armazenar (*data centers*) tais dado e o quanto é importante manter a sua segurança (MARQUESONE, 2016).

VOCÊ O CONHECE?

Alan Turing, conhecido como o pai da computação moderna, foi um cientista da computação britânica. Através de seus experimentos ele foi capaz de criar a "máquina de Turing", princípio do computador moderno. Seus esforços vieram para quebrar códigos alemães durante a segunda guerra mundial. Seu trabalho, sem dúvida, impactou não só o *hardware* que temos hoje, mas também toda a Computação, incluindo a Segurança da Informação (BERNARDO, 2015).

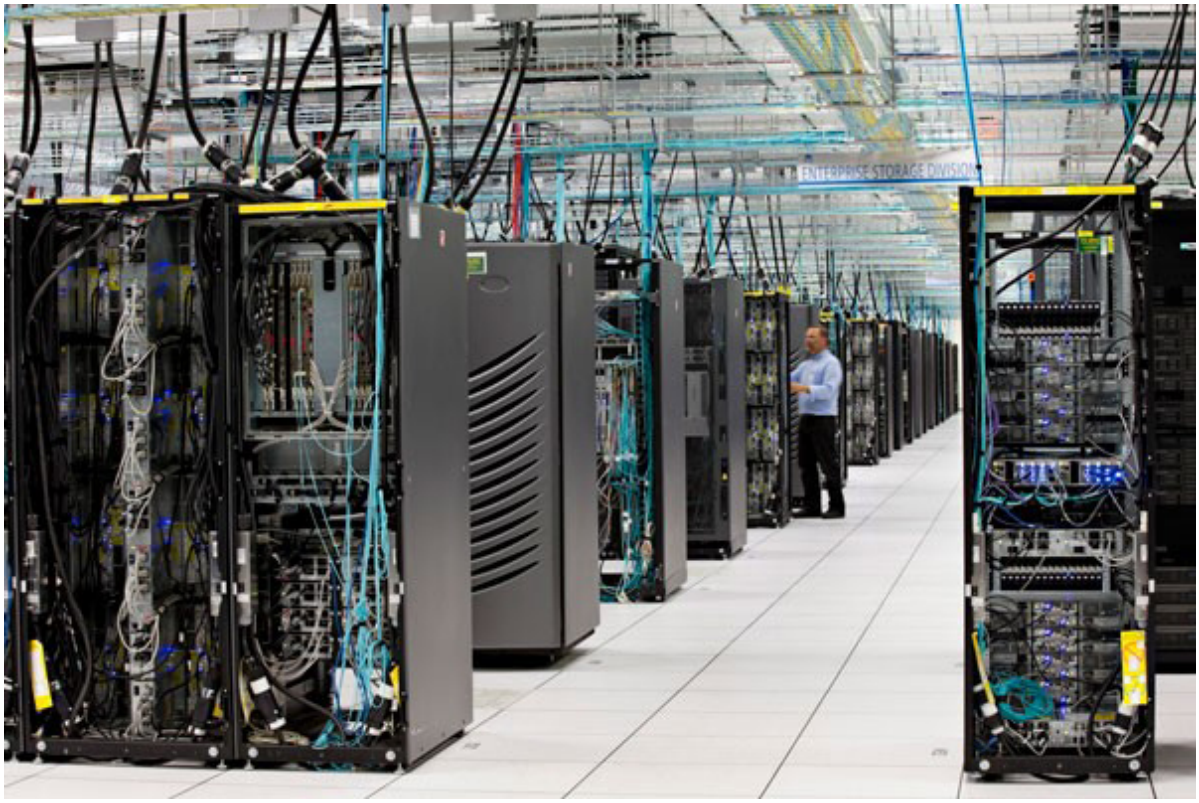


Figura 2 - Data center (servidor de armazenamento). DellEMC Durham – Reino Unido.
Fonte: KLETTKE, 2018.

A nível de comparação, se formos paralelizar esse número com o de pessoas existentes no planeta, que é de aproximadamente 7 bilhões de pessoas, esse número saltaria para 1 trilhão. Além disso, nem foram levados em consideração os dados produzidos por máquinas, a exemplo da área da *Internet* das Coisas (*Internet of*

Things – IoT), que pode ser um dado gerado por um sensor de movimento ativado em sua casa, o qual gera uma notificação que você recebe via *software* (MARQUESONE, 2016).

Em relação à variedade de dados, eles podem ser semiestruturados, não estruturados e estruturados. Dentro desse universo, o que mais nos interessa são os dados estruturados e dentre vários destacamos o banco de dados relacional. Para termos uma noção da complexidade que é armazenar um dado, todos os SGBDs (Sistemas de Gerenciamento de Banco de Dados) devem garantir as propriedades ACID (MARQUESONE, 2016), acrônimo de Atomicidade, Consistência, Isolamento e Durabilidade. A seguir explicamos cada uma delas. Clique nos itens.

Atomicidade	Garante que uma transação, um conjunto de ações, a saber, inserção, alteração, exclusão, seja efetuada por completo ou não. Por exemplo, numa transação de compra de ingresso, você efetuou o pagamento e, por consequência, um ingresso deveria estar disponível. Mas, imagine a situação na qual ao efetuar o pagamento, o seu *notebook* acabasse a bateria. Possivelmente, você só pagaria o ingresso e não haveria tempo de o sistema lhe gerar um convite pago.
Consistência	As tabelas de um banco de dados são interconectadas e devem garantir que as suas restrições de integridade sejam respeitadas. Um exemplo, a integridade referencial, ou seja, uma tabela se relacionando com outra. Se ao tentar incluir um registro na tabela Filhos e informar que o "X" é o pai, tem-se que garantir que na tabela de Pais existe uma linha (registro/tupla) "X". Caso não tenha, informaremos dados inconsistentes. Espera-se o registro pai "X", mas ele não existe. Alguma coisa está errada, ou no nome do pai ou incluir, primeiramente, o nome dele antes e incluir o filho.
Isolamento	É o ato de que uma transação não conheçe outras transações, ou seja, uma transação não irá interferir em outra. Em uma compra *on-line*, pense na complexidade que seria ao tentarmos esperar a transação de outro cliente enquanto estivéssemos comprando. Com certeza, com essa abordagem ganhamos maior desempenho e mais agilidade.
Durabilidade	É o ato de garantir que as transações ocorridas com sucesso tenham seus dados armazenados. Quando salvamos alguma informação em um banco de dados espera-se acessá-lo posteriormente várias vezes. Essa propriedade garante que os dados serão duráveis, ou seja,

estarão disponíveis para acesso por muitos anos. Por exemplo, dados relativos a atendimento médico em uma empresa devem armazenar tais informações pelo menos por 20 anos.

A seguir, falaremos sobre Segurança da Informação, acompanhe!

1.2 O que é Segurança da Informação (SI)?

A *Internet* conecta todos nós em um espaço único, o ciberespaço ou rede mundial de computadores. Lá, trocamos informações entre diferentes pessoas, entre governos, entre entidades por um meio heterogêneo de dispositivos. Todavia, ao nos conectarmos nesse meio de comunicação estamos sujeitos a riscos (Galvão, 2015).

Para nos conectarmos ao ciberespaço precisamos de meios físicos, sistemas operacionais, sistemas, protocolos etc. e muitos deles não são seguros por padrão. Para compreendermos melhor o que vem a ser toda essa interconexão temos que relembrar o conceito básico de comunicação (KIM; SOLOMON, 2014). A comunicação, de modo geral, é dividida da seguinte forma, como vemos a seguir. Clique nos itens.

Emissor	Responsável em enviar as informações. Por exemplo, pode ser uma pessoa querendo mandar um *e-mail* para alguém.
Canal de comunicação	É o meio físico pelo qual a informação é trafegada. Exemplo: *wi-fi*, ondas de rádio, *Internet* etc.
Protocolo	É uma linguagem comum para quem emite e para quem recebe a informação. Por exemplo, estamos usando a língua portuguesa.
Receptor	Recebe a informação passada usando todas as definições anteriores.

Para o nosso contexto da SI, por exemplo, as informações trafegadas podem usar um canal de comunicação da *Internet* com o protocolo TCP/IP. Ele é o protocolo de transferência mais comum na *Internet*, ou seja, qualquer máquina compreende tal "idioma". O TCP/IP (*Transmission Control Protocol/Internet Protocol*) é divido em quatro camadas, a saber: **Aplicação, Transporte, *Internet* (ou Rede)** e **Interface de Rede** (KIM; SOLOMON, 2014). Cada uma dessas camadas irá interagir com diferentes abstrações como a baixa, mais compreensível a nível de máquina ou alta, mais compreensível para o ser humano.

Para se ter uma ideia, a Interface de Rede irá se comunicar a nível de *hardware*, enquanto a camada de Aplicação seria, por exemplo, um *software* de gerência de recursos humanos. Os dados trafegados chegam à camada mais inferior (Interface de Rede) e vai repassando as informações até a camada mais abstrata, a de Aplicação. Além disso, dentro de cada camada há inúmeros outros protocolos, cada qual com suas particularidades. Observe a figura abaixo.

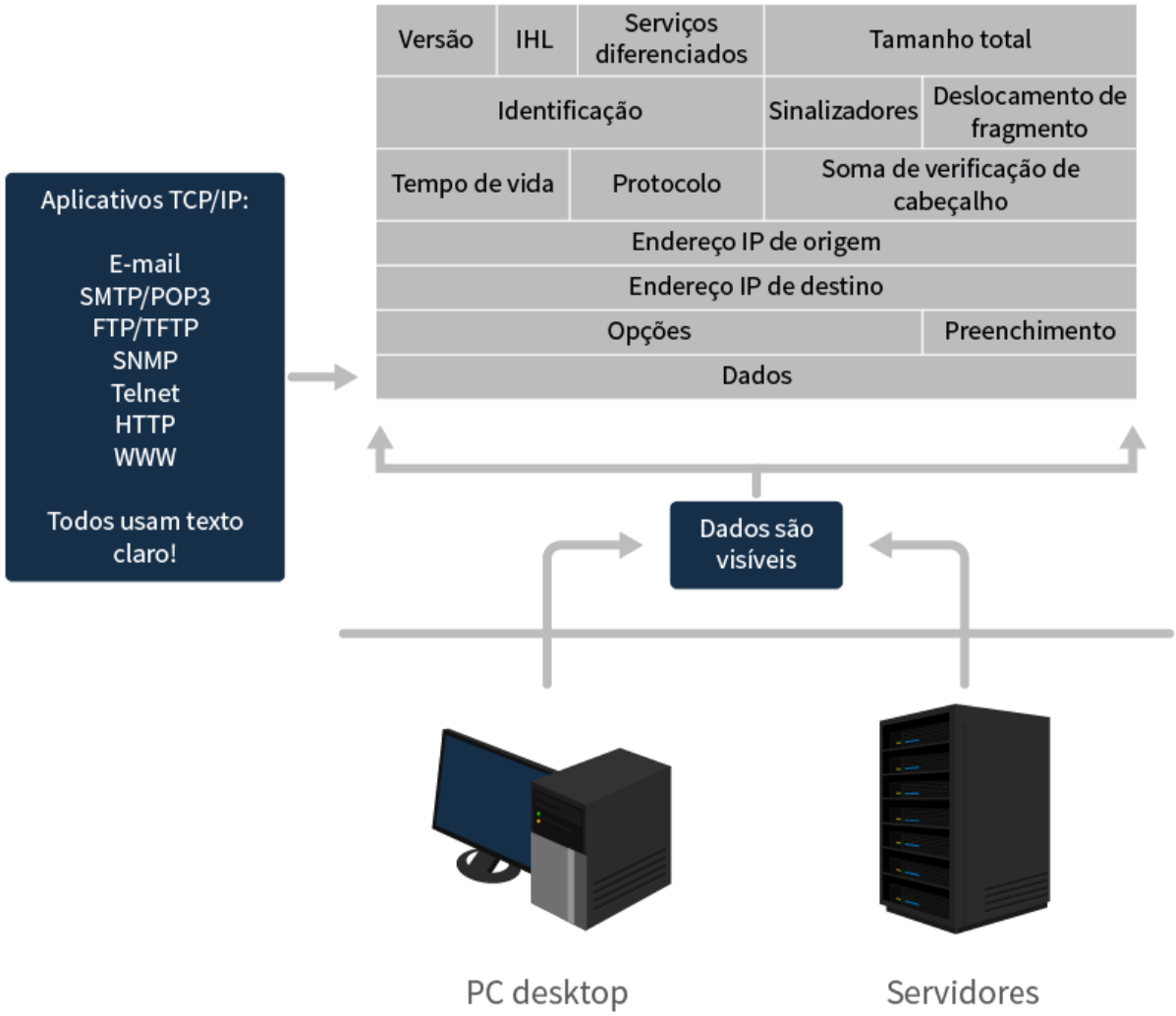


Figura 3 - Pacote de dados transmitidos entre máquinas.
Fonte: KIM; SOLOMON, 2014, p. 5.

Através do protocolo TCP/IP na camada de Aplicação (caixa situada à esquerda na figura) temos alguns exemplos de protocolos. Como exemplo bem simples, podemos destacar o HTTP (*Hypertext Transfer Protocol*). Ele é muito utilizado na comunicação *webservice* (serviços *web* – *REST/SOAP*), porém, as informações transmitidas são visíveis no momento da comunicação (texto claro).

Pensando em segurança, qualquer pessoa poderia interceptar essa informação e utilizá-la para o mal (KIM; SOLOMON, 2014). Outra vulnerabilidade é que os dados na *Internet* passam, em sua grande maioria, por cabos, também conhecidos como *backbone* (espinha dorsal da *Internet*).

VOCÊ SABIA?

Backbone é uma rede de cabos ópticos que visa a conectar diferentes servidores/equipamentos de diferentes localidades ao redor do mundo. Ela é conhecida também como a espinha dorsal da *Internet*. É possível ver a configuração do cabeamento atual no *site*:

https://www.submarinecablemap.com/ (https://www.submarinecablemap.com/).

A partir dessa premissa, há uma grande necessidade de proteger as informações geradas e em meio a essa necessidade nasce a Segurança da Informação (SI). Podemos defini-la como sendo um conjunto de tarefas que visa à proteção de sistemas de informação (sistema operacional, *softwares*, *hardwares* etc.) juntamente com seus dados. Veremos posteriormente que não precisaremos reinventar a roda, uma vez que podemos seguir normas/padrões internacionais que abrange a SI.

1.3 Conceitos e termos utilizados na SI

Antes de estudarmos mais sobre a SI vamos conhecer algumas definições/termos que são bastante utilizados. Muitas dessas definições/termos são oriundas de normas da área de Segurança da Informação (HINTZBERGEN *et al.,* 2018). *A priori,* as normas são um conjunto de padrões de boas práticas e a seguir apresentamos alguns desses termos.

- **Análise de informação** - é um mapa de como uma entidade/organização mantém a sua informação. Ou seja, como as informações trafegam dentro da organização;
- **Ativo** - tudo que gere valor para uma organização, desde *hardware*, sistemas, pessoas e até informações. Possui uma ampla abrangência e, em sua grande maioria, é alvo de diferentes tipos de ataques;
- **Ataque** - visa a corromper, roubar, extinguir, acessar todos os ativos de uma organização. Como é de se esperar, por ser algo tão importante de uma instituição, acaba se tornando um alvo muito fácil;
- **Não repúdio** - impossibilita negar qualquer tipo de operação, serviço ou ação que tenha sido feita sobre a informação. Por

exemplo, informar que o relatório não foi gerado por falta de um arquivo que não foi recebido. Outro exemplo são as ações que um piloto de avião faz em relação a todos os controles da aeronave. Se o piloto informar que tal instrumento não estava funcionando é possível verificar com exatidão se tal instrumento estava em pleno funcionamento no momento em que ele realizou a ação. Em outras palavras, é impossível mentir sobre o que ele fez, pois é possível realizar uma auditoria;

- **Autenticidade** - assegura que o usuário/informação é quem realmente diz ser. Garante que o usuário terá acesso as suas informações e que deixará longe qualquer pessoa não autorizada;
- **Diretriz** - metas ou ações a serem tomadas para se chegar a um objetivo. Esses objetivos são definidos nas políticas de cada organização;
- **Negação de serviço** - DoS (*Denial of Service*) visa a inutilizar o servidor com inúmeras requisições, causando a sua queda de serviço;
- ***SQL Injection*** - é um tipo de ataque que interage com a base de dados via *SQL*. A inclusão de *SQL* se dá por meio de entrada de dados de formulários dos sistemas;
- ***Phishing*** - rouba informações por meio de um *e-mail* que, aparentemente, é confiável. Nele, alguém (um terceiro), se fazendo passar por alguma empresa, por exemplo, requisita uma série de informações (CPF, número de cartão de crédito etc.) que o usuário deve confirmar para ter acesso a alguma vantagem. Há casos em que até se disponibiliza um *link* com uma cópia exata do *site* para obter dados de acesso;

Figura 4 - Phishing de sua ligação com e-mails.
Fonte: Shutterstock, 2019. http://mediapool.fabrico.com.br/index.php/tagueadas-02/shutterstock_120992377

- **Política** - um padrão definido pela organização. Tais políticas podem ser baseadas em normas ou com base em experiências de boas práticas internas/externas;
- **Gestão da informação** - define como a instituição gerencia suas informações, desde a sua coleta até o seu descarte. Aqui, há a identificação do valor da informação;

VOCÊ QUER VER?

Uma das séries mais bem adaptadas para representar o mundo da Segurança da Informação é *Mr. Robot*, dirigida por Sam Esmail. Nela, um jovem engenheiro de segurança (interpretado por Rami Malek) é protagonista de uma série ações envolvendo esse tema, como acesso a dados, espionagem etc. A série entrou no ar em 2015 e possui até o momento três temporadas.

- **Processo** - grupo de atividades relacionadas;
- **Responsabilidade** - ato de se delegar atividades e tomada de decisões;
- **Sistema de Gerência da SI** - ato de gerenciar a SI na organização. Ela envolve desde políticas até suas atividades e seus processos;
- **Terceiro** - pessoa ou entidade que não faz parte do meio.

1.4 Os princípios fundamentais da SI

A Segurança da Informação visa a proteger as informações, deixando-as seguras de diferentes ameaças. Para que isso ocorra, a SI deve possuir uma garantia de princípios que permitem tal ação. Basicamente, a SI está fixada sobre três alicerces (princípios) (KIM; SOLOMON, 2014), como vemos a seguir. Clique nas abas.

Disponibilidade

É a garantia que o usuário terá acesso à informação sempre que necessitar. Se o serviço é essencial, ele deverá estar disponível durante todo o tempo. Muitas vezes, existe um contrato informando a porcentagem de disponibilidade que um sistema deverá manter, por exemplo, de que ficará on-line 98% do tempo. Imagine que você tenha um site de compras e se ele não ficar disponível para seus clientes 24 horas você terá prejuízos.

Integridade

Podemos dizer que manter dados íntegros e significa que a informação deverá permanecer intacta sobre qualquer circunstância de erro. Por exemplo, se você estiver fazendo uma transferência bancária e a energia for interrompida, o sistema deverá ter inteligência suficiente para voltar à operação desde onde você parou, antes da ocorrência do incidente. Ou seja, aquela transferência não será efetivada até que você possa retomá-la e, então, concluí-la.

- **Confidencialidade**

Pessoas com autorização terão acesso à informação. Imagine se qualquer pessoa pudesse acessar a sua conta bancária. Nenhum sistema seria seguro, pois todos acessariam qualquer coisa. Por esse motivo é que existe a confidencialidade, ou seja, somente você terá acesso à determinada informação.

Muitos autores se referem a esses três termos como o triângulo ou tríade, ou simplesmente CID, um acrônimo de Confidencialidade, Integridade e Disponibilidade. Sempre que estivermos falando sobre segurança de informações teremos que ponderar esses três princípios. Após a sua definição é possível definir estratégias e controles para a segurança dos dados.

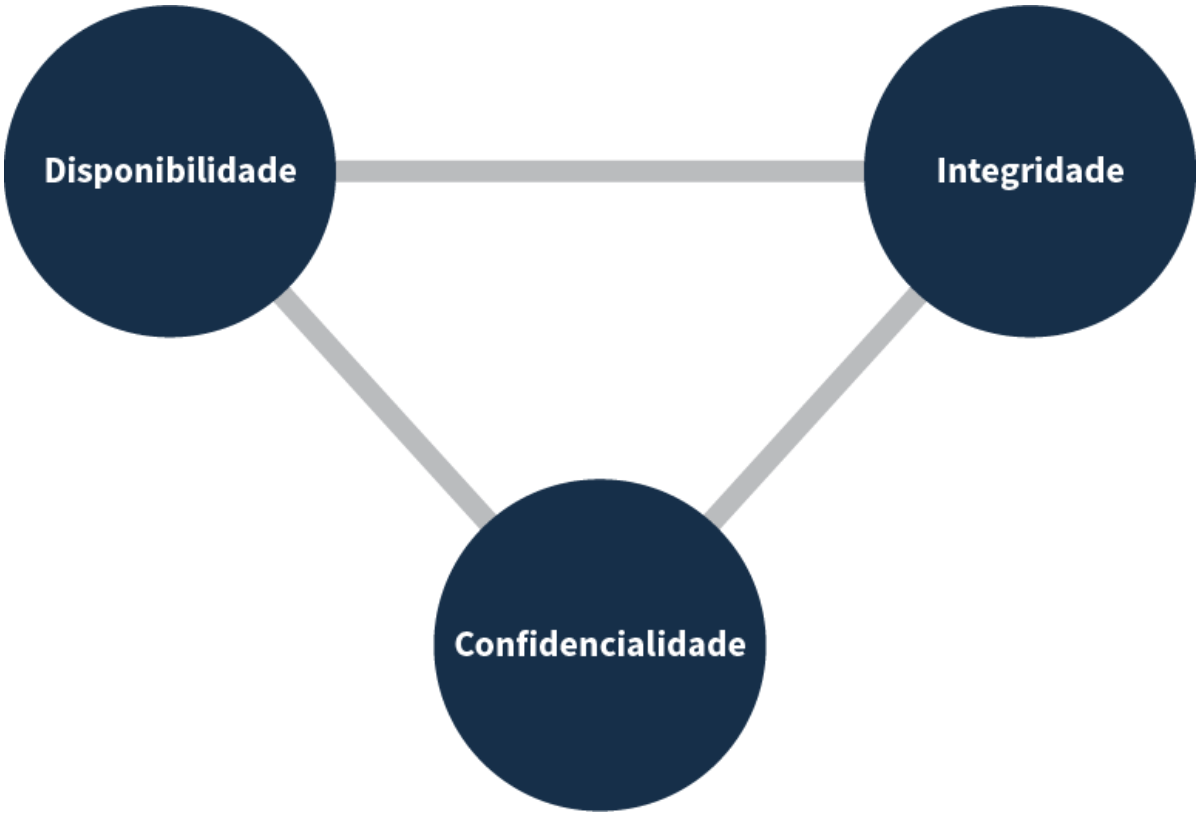


Figura 5 - Tríade da Segurança da Informação.
Fonte: Elaborado pelo autor, 2019.

A seguir, descreveremos mais alguns pontos importantes sobre cada um dos princípios.

Disponibilidade - acredito que esse seja o termo que mais nos afeta uma vez que, diariamente, temos acesso a diversos serviços. Pense sobre o pacote de dados de seu celular, por exemplo, que você adquiriu para acessar a *Internet* em qualquer local, mas certo dia você acabou viajando para uma cidade vizinha que não tinha sinal e sua *Internet* não funcionou. O que adiantou você pagar um valor elevado se quando precisa ele não está disponível? A qualidade desse serviço é expressa pelo tempo disponível ao usuário (KIM; SOLOMON, 2014). Vejamos algumas dessas medidas de tempo a seguir.

- Utilização - tempo total que permanece acessível. Ele é medido dentro do mês levando em consideração horas, minutos e segundos;
- Paralisação - tempo total sem acesso. Ele possui a mesma medida da utilização, porém, quanto maior o tempo, menor é a qualidade do serviço;
- Disponibilidade - ela pode ser calculada usando uma simples equação: (quantidade total de utilização) / (quantidade total de utilização + quantidade de tempo paralisado);
- Tempos médios - todos nós sabemos que é impossível que algo fique disponível eternamente, uma vez que sempre haverá riscos e falhas. Para analisarmos a qualidade de um sistema devemos observar os seguintes tempos médios, como vemos abaixo.
  - Tempo médio para falha (MTTF – *Mean Time to Failure*) – como o próprio nome diz, estamos olhando a quantidade de tempo que ocorre entre uma falha e outra. Quanto menor for esse tempo, pior será o serviço e sua qualidade. Podemos considerar aqui, o tempo de vida útil de um componente ou um sistema como todo;
  - Tempo médio de reparo (MTTR- *Mean Time to Repair*) – sabe-se que falhas podem ocorrer, mas quando acontecer, qual será a quantidade de tempo será necessária para restaurar o sistema? Imagine que você está em uma altitude/velocidade de cruzeiro em um avião. Você sabe que o tempo médio para falhas daquele avião é de muitos anos, mas o tempo de reparo pode levar dois dias. Ou seja, dependendo do tipo de serviço, o reparo deve ser imediato;
  - Objetivo de tempo de recuperação (RTO – *Recovery Time Objective*) - é o tempo que se leva para recuperar e retomar o sistema. Imagine a seguinte cena: você tem um sistema de gestão de recursos humanos e ocorreu um erro em um cadastro. Você sabe qual é o problema e o tempo de reparo é de apenas um

minuto, porém, para deixar disponível o sistema aos seus usuários você levará 30 minutos. O tempo extra está relacionado à reinicialização do servidor físico, colocar o servidor de aplicação *on-line*, subir uma nova versão do seu sistema etc. Perceba que não é só ter um reparo rápido, mas também considerar o tempo que levaremos para disponibilizar o serviço aos usuários.

Como dito anteriormente, existe um contrato entre as provedoras de serviço e seus clientes e um tempo de reparo é exigido por contrato. Por exemplo, dentro de um mês e com disponibilidade de 99,93% quer dizer que haverá 30 minutos dedicados aos reparos;

Integridade - esse princípio lida com a qualidade dos dados. Um dos bens mais preciosos de uma organização são os seus dados. Os dados armazenados podem ser ações em uma bolsa de valores, cálculos de projetos secretos, patentes, movimentação bancária etc. Imagine uma agência bancária que não tem controle nenhum de suas informações. Em um dia você poderia estar milionário e em outro ter feito um empréstimo. Nesse princípio de segurança temos que assegurar que os dados são reais, válidos e que não sofreram nenhuma alteração sem autorização (KIM; SOLOMON, 2014);

Confidencialidade - este princípio protege o acesso das suas informações de outras pessoas que não sejam pertinentes. Atualmente, muitas pessoas deixaram de comprar produtos em lojas físicas para comparem produtos *on-line*. Isso se dá pela praticidade, pelo bom preço, pelas opções de produto, tipos de entrega etc. Porém, pode acontecer de que sejam expostos seus dados pessoais, como número de cartão de crédito e CPF, por exemplo, a *sites* falsos/terceiros. Em consequência disso, outras pessoas poderão se passar por você e realizar novos débitos, por isso, a confidencialidade é bastante crítica, visto que terceiros podem assumir nossa identidade e causar grandes transtornos. Um termo bastante usado para esse assunto é a Engenharia Social, em que pessoas são capazes de obter qualquer tipo de informação. Logo, medidas devem ser criadas para minimizar tais ataques (KIM; SOLOMON, 2014), dentre as quais podemos ver abaixo.

- Treinar funcionários quanto a ataques de Engenharia Social respeitando padrões e procedimentos estabelecidos na instituição;
- Definir controles de segurança para TI (Tecnologia da Informação);
- Adicionar proteção nas diferentes camadas de infraestrutura da TI. Tal tipo de cuidado pode evitar inúmeros tipos de ataques;
- Reavaliar a segurança em servidores e na infraestrutura observando nossas brechas;
- Monitorar todos os dados que entram e saem;
- Utilizar *softwares* adequados para barrar vírus, *trojans* etc.;
- Introduzir novas formas de autenticação, não só por senha. Mesmo que seja por senha, é preciso aumentar o número de dígitos, envolvendo letras, número, caracteres especiais etc.;
- Preocupar-se com erros nos *softwares*, protegendo suas entradas (campos) e acesso, como o *SQL Injection* e a negação de serviço.

Não permitir o acesso aos dados é só uma etapa desse processo. Deve-se realizar uma série de controles com base em normas, a exemplo da ISO 27001. Vejam os exemplos:

- criar uma política/norma que esteja ligada diretamente com os objetivos da organização para uma maior proteção/manipulação dos dados;
- classificar os dados e garantir que eles recebam os devidos cuidados. Nesse exemplo, devem ser criados controles por toda a infraestrutura de TI;
- adicionar a criptografia nos dados. Esse recurso permite que mesmo que haja acesso a tal informação, o conteúdo não será compreendido. Aqui, se pode criptografar todos os dados da instituição que trafegam na *Internet*, assim como os seus dados;
- restringir o número de acesso a sistemas críticos.

Por exemplo, é bem possível que você já tenha enviado dados pessoais por *e-mail*. Essa é uma péssima opção. Os dados trafegados por *e-mail*, dependendo do provedor, não possuem nenhum tipo de segurança. Em outros casos, o próprio uso de Inteligência Artificial pode ler o conteúdo de seu *e-mail*. Para contextualizar, o próprio Google possui frases prontas no final do *e-mail* para que você responda de forma rápida e perceba que as respostas estão de acordo com o conteúdo do *e-mail*. Se o corpo do *e-mail* contém uma informação de certo agendamento, no final, na frase gerada pela Inteligência Artificial, haverá textos como: "Confirmado", "Não posso nesse dia", "Obrigado" etc.

Sempre desconfie e nunca passe seus dados a ninguém ou a *sites* desconhecidos. Antes de realizar qualquer compra *on-line* verifique se a empresa é séria ou se aquilo é algum golpe. Lembre-se de que as pessoas pegam seus dados a partir de uma isca, um produto muito barato, serviços com recursos ilimitados etc. Fique sempre atento!

Ao observar os princípios da Segurança da Informação, perguntamos quais domínios são afetados dentro da TI (KIM; SOLOMON, 2014). Em resumo, pode-se dizer que são sete, como vemos a seguir. Clique nas abas.

Usuário

São as pessoas que acessam a informação dentro de uma organização. Aqui nos preocupamos com papéis (tipo de usuário) que podem acessar determinadas áreas do sistema; outro aspecto é a responsabilidade (manter dados confidenciais), em que o usuário se relaciona com ativos de uma empresa, por exemplo, dados pessoais, dados bancários etc.

Estação de trabalho

É o equipamento pelo qual o usuário da organização se conecta as informações. Nesse nível, também nos preocupamos com papeis e responsabilidades.

LAN (Local Area Network)

É a rede local da organização. Grande parte dos dispositivos está conectada a essa rede. Aqui, há uma gama de diversos itens físicos, como cabeamentos, *switch*, roteador, servidores de impressão, pontos de acesso à rede etc., bem como a parte lógica: *backups*, administração de sistema etc. Nesse nível também há papeis e responsabilidades.

- ***LAN/WAN***

  Ligação a uma rede externa. Nesse momento, abre-se uma grande possibilidade a ataques.

- ***WAN (Wide Area Network)***

  Possibilita a conexão de locais remotos. Várias empresas oferecem conexões mais rápidas, como *backbones* (espinha dorsal da *Internet* - fibra óptica), *LAN* metropolitana etc.

- **Acesso Remoto**

  Permite que usuários remotos acessem a infraestrutura de TI da organização.

- **Sistema**

  Manipula os ativos de uma organização. Todos os domínios estarão disponíveis a pessoas autorizadas e autenticadas. Assim como as demais, este é um domínio extremamente crítico, pois todas as informações importantes estão disponíveis.

E dentre todos os domínios, o que carece de maior segurança é o usuário. Como diz o velho ditado, "errar é humano" e independentemente da organização ou domínio, se existir uma interação humana, um erro é potencialmente aceitável dado que um usuário é imprevisível.

1.5 Hexagrama Parkeriano

O Hexagrama Parkeriano é outra definição dos princípios da Segurança da Informação. Apesar de possuir os mesmos três atributos do CID, ele ainda acrescenta outros três atributos (HINTZBERGEN *et al.*, 2018). Logo, o hexagrama Parkeriano é definido pelos itens a seguir. Clique e veja.

Confidencialidade.

- Posse ou controle.
- Integridade.
- Autenticidade.
- Disponibilidade.
- Utilidade.

Como discutido anteriormente, já conhecemos os termos da CID - Confidencialidade, Integridade e Disponibilidade. Agora, veremos sobre os outros três termos conhecidos do Hexagrama Parkeriano.

Posse ou controle - o usuário pode ter o controle da informação. Um exemplo bem clássico é o furto de um cartão de crédito. O usuário poderá entrar em contato com a sua operadora e cancelar o cartão imediatamente. Dizemos posse ou controle quando o usuário tem o domínio/direito de uso da informação. Nem sempre esse tipo de controle é real. Já vimos em noticiários que instituições financeiras, operadoras de *telemarketing*, dentre outros, vendem as informações de seus clientes para outros concorrentes. Infelizmente, não há um controle efetivo sobre isso. Ao certo, não se sabe até quanto nossos dados são mantidos de forma segura;

Autenticidade - é o princípio que garante que o usuário que deseja o acesso é realmente quem ele afirma ser. É preciso tomar medidas para que se garanta a confiabilidade de acesso, a exemplo da assinatura digital. Por meio dela o usuário poderá ter um *token* (semelhante a um *pendrive*) e inserir em uma entrada USB. Outro exemplo bem comum em caixas eletrônicos é a autenticação via biometria. Há, ainda, a autenticação em duas etapas, bastante utilizado, em que você acessa seu *e-mail* informando a senha, como de costume e, em seguida, é requisitado um código que será enviado por SMS, via *WhatsApp*, via assinatura digital etc.. Desta forma, garante-se mais um nível de segurança na sua autenticação;

Utilidade - identifica qual é a importância da informação. Uma vez compreendido a importância pela qual o dado é para a organização pode-se tomar maiores medidas de segurança, a fim de garantir a sua proteção.

VOCÊ QUER LER?

"Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito" (2015), de Richard A. Clarke e Robert K. Knake. O livro aborda o cenário atual da guerra cibernética, ponderando as armas computacionais e seus impactos nos diversos meios, como sociedade, governos, militares etc.

Apesar de o Hexagrama Parkeriano incluir mais três propriedades aos princípios clássicos (CID), eles não se sobrepõem. Podemos dizer que são complementares, mas usa-se mais o CID como uma referência para definir os princípios da Segurança da Informação.

CASO

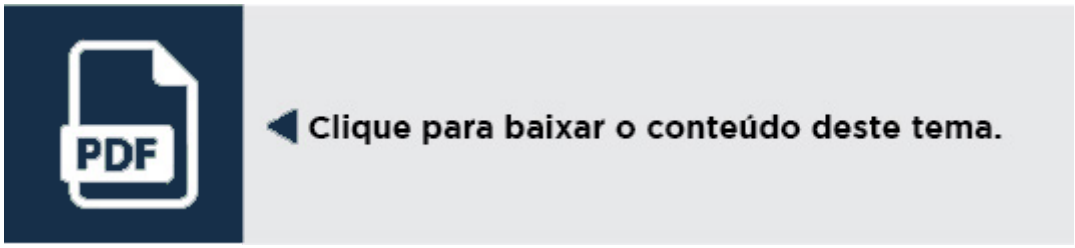
Um dos vírus que mais conhecidos do mundo foi o Melissa. O seu criador David Smith, estudante de computação de 30 anos, quis prestar uma homenagem a uma dançarina de uma boate chamada Melissa. O motivo pelo qual ficou tão famoso foi por ser o primeiro vírus do mundo que se reenviava e se autocopiava. Esse vírus foi difundido via *e-mail* com uma grande rapidez, por meio de um arquivo .DOC anexo com uma mensagem: "Aqui está o documento que você me pediu, não mostre para mais ninguém.". Em consequência, 20% de todos os computadores do mundo foram infectados. O vírus também corrompia alguns arquivos inserindo alguns textos de referência da fala de um dos personagens de *Os Simpsons*. O prejuízo causado pelo Melissa está estimado em US$80 milhões, sendo que grandes empresas também foram infectadas, como a própria Microsoft e Intel. Smith, inicialmente, foi condenado a 10 anos de prisão, mas no final aceitou trabalhar para o FBI e sua pena foi reduzida (GOODRICH; TAMASSIA, 2013).

Vimos que o Hexagrama Parkeriano é uma complementação do Princípio da Segurança da Informação. Além disso, ele dá mais detalhes sobre o dado. Ou seja, passamos a conhecer o grau de importância do mesmo. Conhecendo a sua utilidade, propriedade e acesso.

Síntese

Nesta unidade, você teve a oportunidade de:

- A quantidade de dados cresce exponencialmente a cada ano. Devemos nos preocupar com o armazenamento e segurança dos dados;
- Os dados são apenas sequência de *bits*, sem sentido semântico;
- A informação é a caracterização/contexto de um dado;
- Conhecimento é uma interconexão de várias informações;
- Um SGBD (Sistema de Gerência de Banco de Dados) garantem a propriedade ACID - Atomicidade, Consistência, Isolamento e Durabilidade;
- A comunicação envolve: emissor, canal de comunicação, protocolo e receptor;
- Grande parte das comunicações entre computadores/servidores são através do "texto-limpo";
- Os princípios fundamentais da Segurança da Informação são: Disponibilidade, Integridade e Confidencialidade;
- Os sete domínios afetados pela Segurança da Informação são: usuário, estação de trabalho, LAN, LAN/WAN, WAN, acesso remoto e sistema;
- O Hexagrama Parkeriano é uma complementação dos princípios da SI. São eles: Confidencialidade, Posse ou controle, Integridade, Autenticidade, Disponibilidade e Utilidade.



Bibliografia

BERNARDO, H. G. **Alan Turing**: A tragédia de um gênio. São Paulo: Chambel Multimedia, 2015.

CLARKE, R. A.; KNAKE, R. K. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer. São Paulo: Brasport, 2015.

GALVÃO, MICHELE DA COSTA. **Fundamentos de Segurança da Informação**. Pearson, 2015. Disponível em: (https://www.bvirtual.com.br/NossoAcervo/Publicacao/26525)https://www.bvirtual.com.br/NossoAcervo/Publicacao/26525 (https://www.bvirtual.com.br/NossoAcervo/Publicacao/26525). Acesso em: 08 jul. 2019.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à segurança de computadores**. São Paulo: Bookman, 2013.

HINTZBERGEN J. et al. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

MARQUESONE, R. **Big Data**: técnicas e tecnologias para extração de valor dos dados. São Paulo: Casa do Código, 2016.

MR. ROBOT [Seriado]. Direção: Sam Esmail. Produção: Steve Golin, Chad Hamilton, Igor Srubshchik. Nova Iorque: Universal Cable Productions, 2015.

KLETTKE, R. Dell EMC Data Centers Run on Partnership and Teamwork. American Builders Quartelity, 15 jun. 2018. Disponível em: (https://americanbuildersquarterly.com/2018/06/15/dell-emc-data-centers-run-on-partnership-and-teamwork/)https://americanbuildersquarterly.com/2018/06/15/dell-emc-data-centers-run-on-partnership-and-teamwork/ (https://americanbuildersquarterly.com/2018/06/15/dell-emc-data-centers-run-on-partnership-and-teamwork/). Acesso em: 08 jul. 2019.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação.** São Paulo: LTC, 2014.

SÊMOLA, M. **Gestão da segurança da informação**. Elsevier Brasil, 2014.

TELEGEOGRAPHY. **Submarine Cable Map**, 2019. Disponível em: (https://www.submarinecablemap.com/)https://www.submarinecablemap.com/ (https://www.submarinecablemap.com/). Acesso em: 27 jun. 2019.