



# SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 2



Prof. Douglas Eduardo Basso



## TEMA 1 – FRAMEWORKS DE GESTÃO E APOIO À SEGURANÇA DA INFORMAÇÃO

Atualmente, a área de segurança de informação de uma organização precisa ser bem desenvolvida. É desejável que as organizações utilizem os recursos de TI com maturidade, com uma boa governança de TI. Os frameworks são excelentes ferramentas para auxiliar as organizações na implementação de modelos, métricas e medidas quando se trata de segurança da informação, pois trazem consigo as melhores práticas.

Um framework de gestão e apoio à segurança da informação nada mais é do que uma série de procedimentos e guias utilizados para a definição de políticas e processos relacionados ao implemento e ao gerenciamento, de forma contínua, de controles de segurança da informação em um ambiente organizacional.

Os frameworks funcionam como uma espécie de enciclopédia, apresentando as melhores práticas de governança de segurança da informação. Sua implementação traz vantagens e benefícios, entre os quais podemos citar os que se seguem.

- Contratação de colaboradores: recrutar novos funcionários que tenham conhecimento sobre determinado framework pode ser um pré-requisito, pois ajuda a diminuir custos com treinamento, facilitando também na adaptação do novo colaborador aos processos e práticas desejadas pela organização.
- Diminuição de custos: para reduzir custos, recomenda-se controlar as vulnerabilidades da área de TI; criar mecanismos de redundância e contingência; mitigar possíveis ameaças; e desenvolver análises preditivas. Minimizando esses problemas, é possível estabelecer maior continuidade dos negócios, sem nenhum tipo de interrupção prejudicial às atividades e aos processos de negócio.
- Clareza para comparações: estabelecer comparações com outras organizações é importante para descobrir oportunidades e melhorias de negócio. Aumento de performance, com análise de detalhes sobre a implementação de frameworks em outras organizações, pode ser importante útil para identificar os pontos fortes e fracos de cada



framework, possibilitando coletas mais assertivas (com padrão) em relação à segurança da informação.

- Melhoria da segurança: com a implantação de um framework, há melhoria em segurança, confiabilidade e qualidade dos dados. Afinal, a implementação dos frameworks requer alinhamento com uma série de regras, normas e regulamentos relacionados a todos os tipos de dados que trafegam pelas organizações, melhorando a sua acessibilidade.
- Conformidade: as boas práticas de governança ajudam nos processos de auditoria. São maneiras de garantir uma boa avaliação dos sistemas de informação, com adoção de padrões alinhados com a conformidade, reduzindo os riscos. A área de TI ganha em maturidade e na gestão de riscos.
- Linguagem comum: empresas que utilizam frameworks de segurança da informação podem trocar dados e informações, o que ajuda no diálogo entre as equipes técnicas, criando uma base conceitual e auxiliando na busca por parceiros e na contratação de cursos de aperfeiçoamento para os colaboradores.

Agora que sabemos um pouco sobre os frameworks, vamos conhecer alguns deles ao longo desta aula. Destacamos que alguns são reconhecidos internacionalmente.

## 1.1 CIS Controls

Os controles CIS (Center for Internet Security) são basicamente conjuntos desenvolvidos de práticas recomendadas em segurança cibernética. São ações defensivas que visam minimizar e evitar ataques cibernéticos. Os controles são elaborados por grupos de especialistas de TI, usando como base dados coletados de ataques cibernéticos reais e o estudo de ações eficazes de defesa.

Os controles apresentam grande eficácia, fornecendo um caminho para que as organizações busquem uma defesa cibernética mais robusta, com ações de retorno imediato, que são relativamente curtas, concentrando as atenções quando há risco de alto valor.

A estrutura de controles CIS apresenta 18 recomendações, divididas em categorias (básico, essencial e organizacional).



- Inventário e controle de ativos da empresa: gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos da empresa (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não informáticos; IoT – Internet das Coisas; servidores) conectados à infraestrutura física, virtual e remotamente, considerando ainda aqueles em ambientes de nuvem, de modo a descobrir com precisão a totalidade de ativos que precisam ser monitorados e protegidos dentro da empresa. Esse processo também apoia a identificação de ativos não autorizados e não gerenciados para removê-los ou corrigi-los.
- Inventário e controle de ativos de software: gerenciar ativamente (inventarie, rastreie e corrija) todos os softwares (sistemas operacionais e aplicações) na rede, para que apenas softwares autorizados sejam instalados e executados – softwares não autorizados e não gerenciados devem ser encontrados para impedir a sua instalação ou execução.
- Proteção de dados: desenvolver processos e controles técnicos para identificar, classificar, manusear, reter e descartar dados com segurança.
- Configuração segura de ativos corporativos e software: estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não informáticos; IoT; servidores) e software (sistemas operacionais e aplicativos).
- Gestão de contas: utilizar processos e ferramentas para atribuir e gerenciar a autorização para credenciais nas contas de usuário, incluindo contas de administrador, bem como contas de serviço para ativos corporativos e software.
- Gerenciamento de controle de acesso: usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégio para contas de usuário, administrador e serviço, considerando ativos e softwares corporativos.
- Gerenciamento contínuo de vulnerabilidade: desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos corporativos dentro da infraestrutura da empresa, a fim de remediar e minimizar a janela de oportunidade de invasores. Monitorar fontes da indústria pública e privada para novas informações sobre ameaças e vulnerabilidades.



- Gerenciamento de registro de auditoria: coletar, alertar, analisar e reter logs de auditoria de eventos que podem ajudar a detectar, compreender ou recuperar-se de um ataque.
- Proteções de e-mail e navegador da web: melhorar as proteções e detecções de ameaças de vetores de e-mail e web, pois elas são oportunidades para que os invasores manipulem o comportamento humano, por meio de engajamento direto.
- Defesas contra malware: impedir ou controlar a instalação, disseminação e execução de aplicativos, códigos ou scripts maliciosos em ativos corporativos.
- Recuperação de dados: estabelecer e manter práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.
- Gerenciamento de infraestrutura de rede: estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) os dispositivos de rede, a fim de evitar que os invasores explorem serviços de rede e pontos de acesso vulneráveis.
- Monitoramento e defesa de rede: operar processos e ferramentas para estabelecer e manter um monitoramento de rede abrangente, com defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuários da empresa.
- Conscientização de segurança e treinamento de habilidades: estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho, a fim de gerar conscientização sobre a segurança e qualificação adequada, de modo reduzir os riscos de segurança cibernética na empresa.
- Gestão de provedores de serviços: desenvolver um processo para avaliar os provedores de serviços que mantêm dados confidenciais ou que são responsáveis por plataformas ou processos de TI críticos de uma empresa, de modo a garantir que esses provedores sejam capazes de proteger as plataformas e os dados de forma adequada.
- Segurança de software de aplicativo: gerenciar o ciclo de vida da segurança do software desenvolvido, hospedado ou adquirido internamente, para prevenir, detectar e corrigir os pontos fracos de segurança antes que eles afetem a empresa.



- Gerenciamento de resposta a incidentes: estabelecer um programa para desenvolver e manter a capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações), de modo a preparar, detectar e responder rapidamente a um ataque.
- Teste de penetração: testar a eficácia e a resiliência dos ativos corporativos, por meio da identificação e da exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um invasor.

## 1.2 NIST CSF

O framework de segurança da informação NIST (National Institute of Standards and Technology) e o CSF (Cybersecurity Framework) são americanos, com versões publicadas pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos. O seu intuito é criar um aprimoramento das capacidades de prevenção, detecção e resposta a diversos tipos de ataques cibernéticos. Nesse framework, os fatores relacionados ao negócio têm um peso maior. Seu enfoque recai sobre médias e grandes empresas, por conta da complexidade de sua concepção.

As empresas têm investido em ferramentas para a automatização e o gerenciamento de riscos de parceiros e fornecedores, monitorando e classificando de forma contínua a segurança da informação, bem como a melhoria contínua de exposições de dados e credenciais vazadas.

O NIST Cybersecurity Framework é formado por três partes principais.

- Núcleo da estrutura: um grupo de atividades e premissas da cibersegurança desejada, com linguagens de fácil entendimento. Orienta as organizações na área de gerenciamento e minimização de riscos de segurança cibernética, complementando metodologias existentes de segurança cibernética e tratamento de riscos.
- Perfil de estrutura: o levantamento de todos os requisitos da organização e o mapeamento de todos os processos organizacionais ajuda a criar um perfil da estrutura. O perfil é utilizado para identificar e priorizar oportunidades de melhoria nos padrões de segurança e mitigar os riscos em uma organização.



- Camadas de implantação da estrutura: apresenta um contexto sobre o modo como a organização observa o gerenciamento de riscos de segurança cibernética, com uma orientação sobre o que dever ser considerado e qual o nível de segurança recomendado para os riscos identificados. É utilizado usualmente como ferramenta de comunicação para a discussão e a classificação de riscos, prioridades e custos relacionados.

O NIST Cybersecurity Framework Core foi criado para oferecer às organizações um guia de atividades necessárias para atingir diferentes padrões de segurança cibernética. Conforme o NIST, o core do framework é formado pelo que se segue.

- Funções: estabelece cinco funções de alto nível. São elas: identificar, detectar, proteger, responder e recuperar. Elas não se aplicam apenas ao gerenciamento de riscos cibernéticos, mas a riscos em geral.
- Categorias: o framework apresenta cerca de 23 categorias divididas dentro das 5 funções. As categorias abrangem a amplitude dos objetivos de segurança cibernética (resultados cibernéticos, físicos, pessoais e comerciais).
- Subcategorias: o NIST apresenta 108 subcategorias divididas em 23 categorias principais. São declarações orientadas para resultados, com considerações que ajudam a incrementar um programa de segurança cibernética.

A Figura 1 apresenta todas as funções e categorias mencionadas.



Figura 1 – Funções e categorias NIST

Função	Categoria	ID
IDENTIFY	Asset Management	ID.AM
	Business	Enironment ID.BE
	Governance	ID.GV
	Risk Assesment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
PROTECT	Identify Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
DETECT	Anomalies and Events	DE.AE





	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
RESPOND	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RC.IM
RECOVER	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Fonte: NIST, 2018.

### 1.3 MITRE ATT & CK

O Mitre (Massachusetts Institute of Technology Research & Engineering) é uma grande instituição americana financiada pelo governo, sem fins lucrativos. Esse instituto vai além da cibersegurança, pois apresenta uma série de inovações na área militar e de computação.

Dentro do instituto Mitre, foi adicionado o ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), em 2013. Trata-se de um braço responsável por enumerar, descrever e categorizar comportamentos de adversários com base em cenários globais reais de segurança cibernética. A



partir dessa compreensão de técnicas de ataque, essa base de conhecimento tem sido útil para a montagem de medidas defensivas e ofensivas.

O framework, para o Mitre, é uma base de conhecimento globalmente acessível de táticas e técnicas adversárias com base em observações do mundo real. A base de conhecimento da ATT&CK é usada para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética.

O framework ATT&CK tem grande valor por conta de uma série de configurações. Qualquer política de defesa de informações pode tirar proveito e buscar a aplicação de bases a partir das diretrizes desse framework. Além de apresentar uma linguagem comum para profissionais de TI, o ATT&CK desenvolve atividades relacionadas com teste de invasão e segurança ofensiva. Assim, contribui com a colaboração entre equipes que atuam na área de segurança da informação. Vejamos alguns exemplos dos valores oferecidos pelo ATT&CK.

- Mapeamento de controles defensivos: aperfeiçoar os controles defensivos a partir da compreensão de como e quando visualizamos as táticas e técnicas de ataque mapeadas pelo ATT&CK.
- Caçada a ameaças: mapear todas as possíveis defesas ajuda o framework ATT&CK a entregar um grande apanhado de aspetos defensivos, fornecendo aos caçadores de ameaças ótimos pontos para encontrar atividades dos atacantes até então não detectadas.
- Investigação e detecção: as equipes que registram incidentes e o grupo de profissionais que atuam na resposta podem usar o ATT&CK para referenciar técnicas e táticas que tenham sido detectadas. Isso serve bom base para o entendimento das forças defensivas e das fraquezas encontradas, sendo possível também validar a mitigação e os controles de detecção. A descoberta de problemas de configuração e outras questões operacionais também é de grande valia.
- Referências de equipe envolvida: é importante considerar parceiros e grupos que podem ser envolvidos e referenciados na descoberta de comportamentos definíveis. Esse processo auxilia no entendimento geral das ameaças relacionadas com a segurança da informação.
- Integração de ferramentas: é desejável criar processos que integrem as diversas ferramentas e serviços de segurança da informação. A busca por



padrões de táticas e técnicas encontrados nesse framework ajuda a melhorar o entendimento das ferramentas, o que leva a uma maior coesão de defesa entre elas.

- Colaboração: o compartilhamento de informações relacionadas a um tipo de ataque em específico é essencial, pois um grupo ou uma parte envolvida pode garantir um melhor entendimento sobre o processo, buscando como referência o framework.
- Equipes de testes e invasão: o planejamento, a execução e os relatórios gerados pela equipe de testes, bem como as atividades relacionadas aos testes de invasão, podem se basear no framework, buscando estabelecer uma linguagem comum, para que defensores e atacantes falem o mesmo idioma.

## 1.4 Security ScoreCard

A Security Scorecard é uma empresa que atua no segmento de segurança da informação. Buscar avaliar a maneira como a segurança cibernética está sendo implementada e executada em organizações e entidades corporativas, por meio de resultados de análises ponderadas de sinais de inteligência de ameaças cibernéticas, com o intuito de gerenciar parceiros, terceiros e controles de riscos de TI.

A plataforma Security Scorecard permite que os usuários acompanhem, visualizem e monitorem, de forma contínua, as classificações de segurança, controlando fornecedores ou organizações parceiras e recebendo informes relacionados à área de cibersegurança, sempre com boletins atualizados. Também fornece acesso a dados e informações relacionados a violações de segurança, com registros claros de problemas, além de um histórico que apresenta a reputação das empresas ao longo do tempo em relação à segurança da informação.

Segundo o Security Scorecard, dentre as diversas coletas de informações da plataforma, podemos citar as que se seguem.

- Coleta ativa: descoberta de serviço, captura de conteúdo, impressão digital, enumeração de configuração, descoberta de certificados, resolução de nomes, nomes e números.



- Coleta passiva: redes dedicadas de observação (*honeypots*), servidor projetado para capturar tráfego malicioso (*sinkholes*), servidor DNS passivo, troca de publicidade, remetentes de spam, despejos de credenciais e e-mails registrados.
- Particionamento de rede: segmentação, falhas, convergência, tolerância, redundâncias e congestionamento.
- Demais registros: configuração incorreta, lags, atrasos e omissão.

## TEMA 2 – INTRODUÇÃO À CRIPTOGRAFIA

A segurança da informação dentro das organizações vem passando por uma série de mudanças nos últimos anos. Esse desenvolvimento decorre do uso massivo de equipamentos de tecnologia, com aumento no processamento de dados. Assim, a segurança da informação se tornou uma área importante e valiosa dentro das organizações, por conta da necessidade de ferramentas para a proteção de arquivos e demais informações armazenadas que trafegam dentro das empresas.

Com a chegada de sistemas distribuídos, acessos compartilhados em diversos sistemas e aplicações, além da maior utilização das redes de computadores e principalmente da internet, surge a necessidade de transmitir dados de forma mais segura. A área de segurança de informação, hoje, dá grande atenção a questões relacionadas às redes de computadores e à internet, sendo utilizadas diversas medidas para desviar, prevenir, detectar e corrigir violações de segurança relacionadas com a transmissão de informações.

Nos últimos anos, os ataques na internet e em sistemas ligados a ela se tornaram mais complexos e sofisticados. As habilidades e os conhecimentos exigidos aos atacantes antes era muito maiores; hoje, com o acesso a diferentes ferramentas, sistemas e técnicas de invasão, os ataques se tornaram mais automatizados, de modo que acontecem com maior frequência e causam maiores danos às organizações.

Com o aumento dos ataques e a maior utilização de internet, foram criados diversos protocolos de comunicações, aplicações e sistemas. Assim, com o crescimento da própria internet a segurança da informação teve que migrar para esse cenário, com acessos web, mensagens eletrônicas, aplicações baseadas em internet, computação em nuvem, entre outras ferramentas. Dentro



desse cenário, a criptografia é essencial para garantir confidencialidade e integridade.

## 2.1 Algoritmos e protocolos de criptografia

Segundo Stallings (2015), os algoritmos e protocolos de criptografia apresentam uma ampla gama de aplicações, segurança de rede e de internet. As técnicas de criptografia são aplicadas de maneira expressiva nesse cenário. Os algoritmos e protocolos de criptografia podem ser agrupados em quatro áreas principais.

- Encriptação simétrica: utilizada para ocultar o conteúdo dos blocos ou fluxos contínuos de dados de qualquer tamanho, incluindo mensagens, arquivos, chaves de encriptação e senhas.
- Encriptação assimétrica: usada para ocultar pequenos blocos de dados, como valores de função chamados *hash* e chaves de encriptação, usados em assinaturas digitais.
- Algoritmos de integridade de dados: usados para proteger blocos de dados, como mensagens, de possíveis alterações.
- Protocolos de autenticação: esquemas baseados no uso de algoritmos criptográficos, projetados para autenticar a identidade de entidades.

## 2.2 Mecanismos de segurança

Segundo Fraga (2019), existem diversos mecanismos e recursos de segurança da informação, entre os quais podemos destacar os que se seguem.

- Controles físicos: barreiras que limitam o contato ou o acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta. Vejamos exemplos mecanismos de segurança que apoiam os controles físicos: portais, trancas, paredes, blindagens e guardas.
- Controles lógicos: barreiras que impedem ou limitam o acesso à informação, em ambiente controlado, geralmente eletrônico, que de outro modo ficaria exposta à alteração não autorizada por elemento mal-intencionado.
- Mecanismos de criptografia: permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. São utilizados para



isso algoritmos determinados e uma chave secreta, para que, a partir de um conjunto de dados, seja possível produzir uma sequência de dados criptografados. A operação inversa é a decifração.

- Assinatura digital: conjunto de dados criptografados associados a um documento, com a função de garantir a sua integridade.
- Mecanismos de garantia da integridade da informação: usando funções de *hashing* ou de checagem, um código único é gerado para garantir que a informação permaneça íntegra.
- Mecanismos de controle de acesso: senhas, palavras-chave, sistemas biométricos, firewalls, tokens e cartões inteligentes.
- Mecanismos de certificação: atestam a validade de um documento ou arquivo.
- Integridade: medida em que serviços ou informações são genuínos, isto é, se estão protegidos contra a personificação por intrusos.
- *Honeypot*: software cuja função é detectar ou impedir a ação de um cracker, de um *spammer* ou de qualquer agente externo estranho ao sistema, enganando-o e fazendo-o pensar que ele está de fato explorando uma vulnerabilidade daquele sistema.

Hoje, existem diversas ferramentas e sistemas que auxiliam na segurança da informação. Vejamos alguns exemplos: antivírus, capturadores de tráfego de rede, firewalls, *proxys*, analisadores de código, scanners de portas de comunicação, filtros *antispam*, *fuzzers* e detectores de intrusão.

## 2.3 Aplicações e cenários de uso de criptografia

A utilização da criptografia é um importante instrumento para garantir a segurança nas redes de computadores. Essa técnica é usada para garantir a segurança nos meios de transmissão. Um cenário de uso interessante de emprego da criptografia são as redes wireless, nas quais os dados transmitidos são codificados. Mesmo que esses dados sejam interceptados, dificilmente serão decodificados. A Figura 2 apresenta os padrões de segurança mais utilizados nas redes wireless.

Figura 2 – Padrões de segurança redes wireless



Crédito: Jaiz Anuar/Shutterstock.

Alguns padrões de criptografia foram criados para as redes wireless, dentre os quais podemos destacar os que se seguem.

- WEP – Wired Equivalent Privacy: padrão de segurança disponibilizado juntamente com o padrão 802.11 em 1999. O comitê 802.11 disponibilizou o protocolo sabendo de suas limitações. O WEP era a melhor opção disponível à época. Foi desenvolvido com o objetivo de garantir que os dados trafegados tivessem segurança parecida com uma rede ethernet cabeada. O WEP utiliza chaves fixas de 64 ou 128 bits, com conceito de Shared Key. Na verdade, desses bits, 24 são do vetor de inicialização (IV) do WEP, restando, no caso do WEP64, 40 bits para a chave, ou seja, apenas 5 caracteres de chave. No WEP128, são 104 bits, 13 caracteres. As chaves devem ser compartilhadas entre os usuários, pois se prestam à criptografia e decriptografia dos dados. O WEP combina o IV com a chave fixa para gerar pseudochaves, que servem para criptografar os dados. Para cada quadro transmitido, é gerada uma nova pseudochave, o que torna a criptografia de cada quadro única.
- WPA – Wi-Fi Protected Access: foi criado para solucionar os problemas do WEP. Pode ser usado com chaves compartilhadas, como no WEP, ou com o padrão 802.1x, e EAP (Extensible Authentication Protocol), que identifica usuários através de certificados digitais. Com o 802.1x, é possível garantir centralização de autenticação, através do Radius (Remote Authentication Dial In User Service). O WPA incorpora um esquema de criptografia conhecido como TKIP (Temporal Key Integrity Protocol), que embaralha os frames utilizando um algoritmo de hash que modifica a chave criptográfica a cada 10 pacotes. O WPA utiliza o





protocolo TKIP para a criptografia dos dados através do algoritmo RC4, sempre tomando as devidas preocupações, como não enviar a chave em texto claro, em parceria com uma política de IV mais inteligente. O WPA pode ser utilizado com uma chave secreta entre 32 e 512 bits.

- WPA2: foi desenvolvido para garantir um nível de segurança ainda maior em comparação ao padrão WPA. Uma grande inovação do WPA2 é a substituição do método criptográfico do WPA pelo método AES-CCMP. O CCMP (Counter-Mode/CBC-MAC Protocol) é um modo de operação em cifragens de bloco. Ele evita que a mesma chave seja usada para a criptografia e a autenticação.
- WPA3: esse padrão reforça a segurança apresentando chaves de 192 bits de tamanho, o que garante uma segurança mais robusta em ambientes corporativos. As chaves de encriptação são maiores, sendo empregadas em organizações que se preocupam com a segurança da informação. Sabemos que, quanto maior a chave, mais robusta é a segurança da encriptação dos dados. As chaves criam uma grande dificuldade para ataques cibernéticos em redes críticas.

### TEMA 3 – HASH

Os hashes são utilizados para fazer a identificação de funções criptográficas. Apresentam as funcionalidades de codificação de dados para concatenar caracteres de maneira exclusiva, gerando uma espécie de carimbo, que serve para garantir a autenticidade dos dados, armazenar senhas de segurança e assinar documentos de maneira digital. Elas só funcionam porque se baseiam em uma série de processos matemáticos e lógicos. É possível inserir qualquer série de dados de entrada e gerar uma cadeia de caracteres de comprimento fixo, os chamados *hashes*.

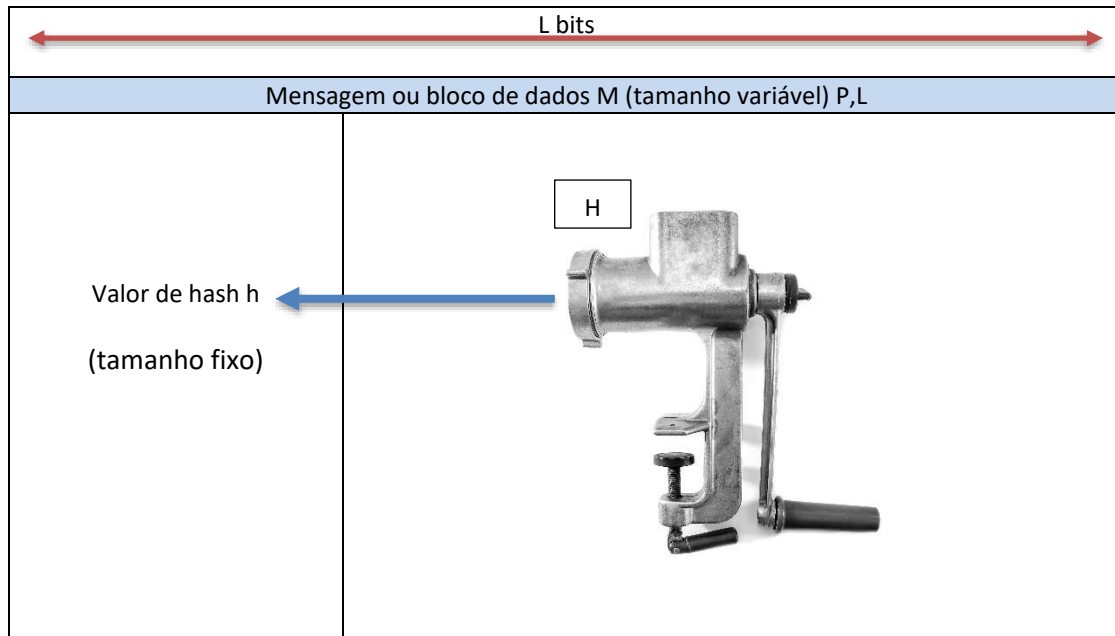
As funções hash recebem uma mensagem de tamanho variável como entrada, produzindo um valor de hash de tamanho fixo. O seu objetivo principal é garantir a integridade de dados. Alterações na mensagem ou nos bits já alteram o resultado da função hash, chamada *mudança no código hash*. De maneira geral, os hash são utilizados para determinar se certos dados da função foram ou não alterados. A tecnologia *blockchain* usa as funções hash como medida de segurança. As criptomoedas também utilizam os hash para a





segurança. A Figura 3 representa a operação geral da uma função hash criptográfica.

Figura 3 – Operação hash criptográfica



Crédito: Tania Kitura/Shutterstock.

### 3.1 História das funções hash

A primeira função hash fazia uma verificação cíclica de redundância, isto é, ela foi gerada para fazer a checagem e a correção de dados transmitidos em rede, como na internet. Foi no ano de 1961 que Wesley Peterson criou a primeira função hash, que recebeu grande aceitação. Inclusive, hoje trata-se de um padrão de mercado.

Esse processo desencadeou novas implementações de funções hash, dentre as quais podemos elencar as que se seguem.

- MD2: uma das pioneiras funções hash criptográficas foi implementada em 1989 por Ronald Rivest. Era uma função muito utilizada na segurança da internet, cuja evolução levou à criação da MD5, padrão muito empregado atualmente.
- RIPEMD: o projeto europeu Ripe criou essa função em 1992, tendo sido implementada para substituir o então hash MD4. É considerada uma função extremamente segura.



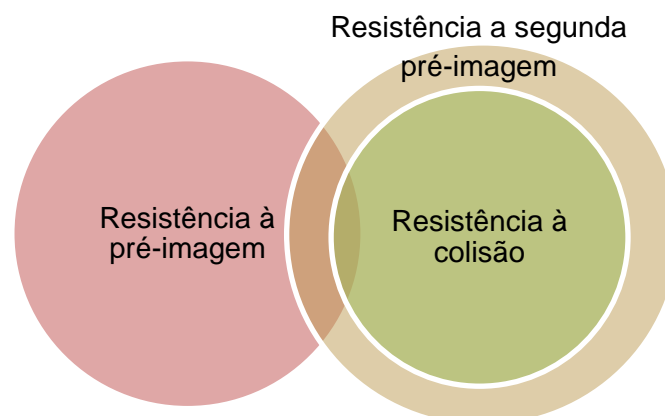
- SHA: é um padrão atual de hash criptográfico. Foi desenvolvido pela NSA em 1993, como componente de um projeto para autenticar documentos eletrônicos. O SHA e suas evoluções são considerados as funções hash mais seguras da atualidade. A criptomoeda Bitcoin utiliza o SHA-256 como tecnologia de segurança.

### 3.2 Propriedades e requisitos do hash

A função criptográfica hash tem uma propriedade praticamente impossível de inverter, com três características que merecem destaque.

- Resistência à pré-imagem: na computação, o valor de dispersão deve ser facilmente encontrado, mas é impossível gerar uma mensagem igual, dado um código, o que protege o valor de entrada dos dados.
- Resistência a segunda pré-imagem: deve ser difícil gerar outra mensagem a partir do seu resultado, com o mesmo valor (hash), burlando a entrada.
- Resistência a colisão: como usamos uma série de funções hash, a integridade é muito importante, de modo que não podem acontecer colisões. Duas mensagens diferentes não podem se valer do mesmo arquivo de hash. A Figura 4 apresenta essas características.

Figura 4 – Características das funções hash



Fonte: Elaborado com base em Stallings, 2015.



### 3.3 Algoritmos hash criptografados

As funções criptográficas hash são utilizadas de maneira ampla em protocolos de segurança como o SSL/TLS e o SSH, e também em outras aplicações que requerem a integridade dos dados.

Dentre as funções criptográficas mais comumente utilizadas atualmente, estão: MD5, Whirlpool, SHA-1, SHA-2 e o SHA-3. As funções hash devem garantir que as mensagens específicas sejam identificadas de maneira única e impossivelmente duplicável.

- MD5 (Message Digest Algorithm 5): função de dispersão criptográfica unidirecional de 128 bits, criada pela RSA, empregada em aplicações e softwares com protocolo de conexão ponto a ponto para checagem e verificação de integridade de autenticação e transferência de arquivos. Foi criada em 1991.
- Whirlpool: algoritmo de criptografia que utiliza codificação livre, sendo um algoritmo utilizado pela Organização Internacional de Padronização (ISO) e pela Comissão Eletrotécnica Internacional (IEC).
- SHA-1 (Secure Hash Algorithm 1): projetado e desenvolvido pela Agência Nacional de Segurança (NSA) dos Estados Unidos e publicado pela NIST. Implementa um valor de dispersão de 160 bits (20 bytes). O SHA-1 integra uma série de aplicações e protocolos de segurança, incluindo o TLS e o SSL. O SHA-1 também é implementado em sistemas de controle de revisão distribuídos, o Git. Através do SHA-1, é possível detectar alteração ou modificação de dados.
- SHA-2 (Secure Hash Algorithm 2): implementado em 2001 pelo NIST, em composição de hash de 224, 256, 384 ou 512 bits. É utilizado em procedimentos de autenticação de pacotes da distribuição Linux Debian e também em assinaturas de mensagens DKIM. Algumas criptomoedas utilizam o SHA-2 para a checagem das transações.
- SHA-3 (Secure Hash Algorithm 3): disponibilizado em 2015 para substituir o SHA-2 e o SHA-1, desenvolvido por Keccak. O SHA-3 é atualmente o algoritmo criptográfico mais seguro e eficiente do mundo. Garante integridade de dados em transações digitais. A sua principal vantagem é que pode ser implementado em uma grande variedade de dispositivos embarcados, móveis, entre outros, permitindo a entrada e a saída de



dados com tamanhos variáveis. Segundo Stallings, a estrutura básica do SHA-3 é um esquema chamado por projetistas de construção em esponja. A construção em esponja tem a mesma estrutura geral de outras funções hash iterativas, recebendo uma mensagem de entrada que é dividida em blocos de tamanho fixo. Cada bloco é processado, por sua vez, com a saída de cada iteração, alimentando a próxima, levando finalmente à produção de um bloco de saída. A Figura 5 apresenta os parâmetros do SHA-3.

Figura 5 – Parâmetros do Algoritmo SHA-3

Tamanho do resumo da mensagem	224	256	384	512
Tamanho da mensagem	nenhum máximo	nenhum máximo	nenhum máximo	nenhum máximo
Tamanho do bloco (taxa de bits r)	1152	1088	832	576
Tamanho da word	64	64	64	64
Numero de rodadas	24	24	24	24
Capacidade c	448	512	768	1024
Resistência à colisão	2112	2128	2192	2256
Resistência à segunda pré-image	2224	2256	2384	2512

Fonte: Elaborado com base em Stallings, 2015.

### 3.4 Aplicações com hash

Existem diversas aplicações com funções hash no cenário de segurança de aplicações da internet. Vejamos algumas delas.

- Autenticação de mensagens: verificação de integridade de mensagens, garantia de que as mensagens recebidas e enviadas foram enviadas exatamente da maneira como foram criadas e disparadas pelos proprietários; mecanismos de autenticação garantem que a identidade do emissor é realmente válida. Segundo Stallings (2015), normalmente a



autenticação de mensagens é alcançada usando o código de autenticação de mensagens (MAC, do acrônimo em inglês para Message Authentication Code), também conhecido como *função de hash chaveada*.

- Assinatura digital: processo parecido com a autenticação de mensagens. Na assinatura digital, é feita a encriptação com a chave privada do usuário. Qualquer outro usuário que saiba a senha pública do usuário pode checar a integridade da mensagem associada à assinatura digital. O tema da assinatura digital será debatido em detalhes nestes estudos posteriormente.
- Carteira de endereços: as carteiras de criptomoedas são uma boa representação de chaves de segurança. Elas usam grandes chaves públicas. Através do uso do blockchain e de funções hash, é possível reduzir o tamanho dessas chaves e ainda criar camadas novas de segurança.
- Mineração de moedas virtuais: a mineração de dados faz um uso intensivo de cálculos de hash, distribuindo os cálculos por todos os equipamentos que fazem parte do sistema distribuído. Os mineradores são responsáveis por milhões de cálculos de hash para a criação de blocos de Bitcoin. As funções hash ainda fazem validações de transações. Os mineradores precisam, cada vez mais, de hardwares potentes e avançados, com maior valor computacional.
- Contratos inteligentes: as funções hash são utilizadas para o versionamento e a validação de contratos inteligentes, marcando a validade de autenticidade. Cada contrato tem um hash exclusivo. Os dados podem incluir: endereços, nomes, endereços de carteira, dados de parceiros, participantes e terceiros. O contrato deve tratar as informações de maneira privilegiada. Apenas os interessados podem visualizar as informações mais sensíveis.

Há uma infinidade de aplicações que utilizam a tecnologia hash, com soluções criadas a partir da evolução de ferramentas de segurança disponíveis na Internet.



## TEMA 4 – CHAVE SIMÉTRICA E ASSIMÉTRICA

Com o aumento de dispositivos conectados em redes e na internet, as pessoas estão cada vez mais inseridas em um ambiente que requer conectividade disponível, eficiente e confiável (Alves, 2021). Assim, é preciso saber se nesse meio há algum tipo de segurança na transição dessa gama infinita de informações trafegadas na rede de um equipamento para outro. Afinal, muitas vezes, o simples ato de estar conectado online, automaticamente e sem saber, acarreta inúmeras transmissões de dados, sem consentimento ou conhecimento prévio do que é absorvido, captado e compartilhado.

Os algoritmos de criptografia são indispensáveis para a segurança da informação. As chaves de segurança possibilitam a verificação, a checagem e a validação das informações. Tais processos podem ser feitos com a utilização de duas técnicas de criptografia: a simétrica e a assimétrica. O controle, o gerenciamento e a distribuição de chaves criptográficas são tarefas bem complexas.

Quando utilizamos a criptografia assimétrica, temos a presença de duas chaves: uma pública e uma privada. Elas não são iguais. Dessa maneira, temos uma assimetria. Já na criptografia simétrica, em geral temos apenas uma chave, que é utilizada tanto no processo de criptografia dos dados, como na etapa de decifração. Dessa forma, temos a mesma chave para a proteção e a abertura de dados.

Na criptografia simétrica, existe um problema relacionado com a distribuição de chaves. Na criptografia assimétrica, não temos esse problema, porém a assimétrica é mais lenta. Quando há um grande volume de dados, a criptografia simétrica é a mais indicada. Dessa forma, podemos dizer que a criptografia simétrica é muito mais rápida. Apesar dos algoritmos serem mais rápidos, não são muito seguros, pois a cifra é compartilhada entre várias máquinas. Já a criptografia assimétrica utiliza uma chave pública para cifrar a mensagem (encriptar, embaralhar, esconder), enquanto a chave privada é empregada para decifrar (desencriptar, desembaralhar, revelar).

Quanto mais complexa a criptografia, mais difícil de ser quebrada. A criptografia tem a finalidade de evitar: falsificação, manipulação, alterações e interceptação de dados enviados. Ela cria um meio de enviar informações de maneira segura. É fundamental que as técnicas computacionais sejam

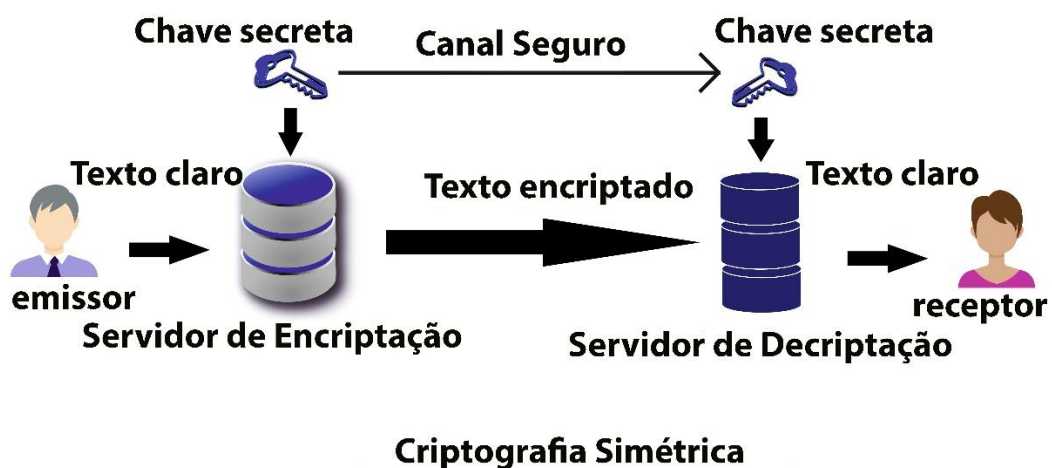


empregadas para atender aos requisitos de segurança da informação. Nesse contexto, temos a atuação dos algoritmos de criptografia simétrica (ou *de chave privada*) e assimétrica (ou *de chave pública*).

#### 4.1 Algoritmos de criptografia simétrica

Os algoritmos de criptografia simétrica apresentam algumas vantagens, entre elas a simplicidade. São fáceis de utilizar e rápidos de executar, considerando o processamento criptográfico. Porém, se as chaves utilizadas forem complexas, a formulação do algoritmo de chave privada é facilitada. A possibilidade de serem interceptadas depende dos recursos computacionais empregados, que fornecem uma boa proteção dos dados. Quanto mais simples for o algoritmo, mais rápida a velocidade de processamento e maior a facilidade de utilização. A figura a seguir apresenta um esquema de criptografia simétrica.

Figura 6 – Esquemático de criptografia simétrica



Crédito: Ujjwal Swami / Shutterstock.

Dentre os algoritmos de criptografia simétrica, podemos destacar:

- AES (Advanced Encryption Standard);
- DES (Data Encryption Standard);
- 3DES (Triple Data Encryption Standard);
- IDEA (Internacional Encryption Algorithm);
- Blowfish;
- Twofish;
- RC (Cifra Rivest); e

- CAST (Carlisle Adams and Stafford Tavares).

## 4.2 Algoritmos de criptografia assimétrica

A criptografia assimétrica foi criada em meados de 1970. Clifford Cocks, matemático do serviço secreto inglês, criou um mecanismo de comunicação usando duas diferentes chaves, uma privada e uma pública, para cifrar os dados. A principal vantagem desse método é a segurança, pois ele dispensa a necessidade de compartilhar chaves. Entretanto, o tempo de processamento de mensagens dos algoritmos de criptografia assimétrica é mais elevado em relação aos algoritmos de segurança simétrica.

Segundo Stallings (2015), o desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução na história da criptografia. Desde o seu início, até os tempos modernos, praticamente todos os sistemas criptográficos têm sido baseados em ferramentas elementares de substituição e permutação. A criptografia de chave pública é baseada em funções matemáticas, em vez de substituição e permutação.

A alta complexidade encontrada na criação e no desenvolvimento de algoritmos capazes de fazer o reconhecimento de chaves duplas, estabelecendo relações entre elas de maneira eficiente e eficaz, cria obstáculos relacionados à necessidade de poder e processamento computacional. A Figura a seguir apresenta um esquemático de criptografia assimétrica.

Figura 7 – Esquemático de criptografia assimétrica







Crédito: Ujjwal Swami / Shutterstock.

A tarefa de criar uma nova técnica de criptografia desafiou muitos criptologistas a encontrarem algoritmos que atendessem aos requisitos da criptografia assimétrica. Dentre os algoritmos de criptografia assimétrica, podemos destacar:

- RSA (Rivest Shamir Adleman);
- ElGamal;
- Diffie-Hellman; e
- Curvas Elípticas (ECC).

Para finalizar a discussão sobre algoritmos de criptografia simétrica e assimétrica, a figura a seguir apresenta aspectos relacionados a esses dois métodos de criptografia.



Figura 8 – Aspectos de criptografia simétrica e assimétrica

Encriptação Convencional	Encriptação de Chave Pública
<p>Necessário para funcionar:</p> <ol style="list-style-type: none"><li>1. O mesmo algoritmo com a mesma chave é usado para encriptação e decriptação</li><li>2. O emissor e o receptor precisam compartilhar o algoritmo e a chave.</li></ol> <p>Necessário para a segurança:</p> <ol style="list-style-type: none"><li>1. A chave precisa permanecer secreta.</li><li>2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se chave for mantida secreta.</li><li>3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.</li></ol>	<p>Necessário para funcionar:</p> <ol style="list-style-type: none"><li>1. Um algoritmo é usado para a encriptação, e um relacionado, para decriptação com um par de chaves, uma para encriptação e outra para decriptação.</li><li>2. O emissor e o receptor precisam ter, cada um, uma chave do para (não a mesma)</li></ol> <p>Necessário para a segurança:</p> <ol style="list-style-type: none"><li>1. Uma das duas chaves precisa permanecer secreta.</li><li>2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se uma das chaves for mantida secreta.</li><li>3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.</li></ol>

Fonte: Elaborado com base em Stallings, 2015.

## TEMA 5 – ASSINATURA E CERTIFICAÇÃO DIGITAL

A assinatura digital é um código digital concatenado com uma mensagem transmitida de maneira eletrônica. Ela faz a identificação do emissor de modo único, com a garantia de integridade da mensagem. A assinatura garante que a mensagem não foi adulterada, ou seja, que ela é íntegra e que o remetente atesta que realmente é quem diz ser, sendo uma prova de autenticidade do emissor, bem como um endosso da origem dos dados.

A partir dos avanços da criptografia de chave pública (criptografia assimétrica), houve a criação e o desenvolvimento de um importante instrumento de segurança: a assinatura digital. Ela apresenta uma série de capacidades relacionadas à segurança, complicadas de implantar de qualquer outro modo.

A autenticação de mensagens protege a comunicação entre duas partes contra um terceiro qualquer. Entretanto, em situações em que nem sempre há confiança total entre emissor e receptor, é imprescindível utilizar recursos a mais, para além da autenticação. Dentro desse cenário, a melhor solução é o emprego de assinatura digital.



A assinatura digital deve cumprir algumas premissas, tais como:

- verificação de autoria, data e hora de assinatura;
- validação e autenticação de todo o conteúdo da mensagem no ato da assinatura; e
- caso haja checagem por terceiros, garantir a validade e a integridade.

Já os certificados digitais permitem superar os problemas relacionados com as assinaturas digitais. Os certificados permitem obter, de maneira segura, as chaves públicas de um determinado utilizador do sistema.

O certificado digital é um processo de garantia de que uma chave pública pertence efetivamente a uma pessoa ou uma empresa. Essa garantia é alcançada combinando a assinatura digital com uma Autoridade Certificadora (CA). Os certificados digitais são arquivos que apresentam uma chave pública e informações pessoais do proprietário. Dessa forma, estabelecem associação entre a identidade do utilizador com a sua chave pública correspondente, sendo validados e assinados de maneira digital pela autoridade certificadora.

Nas seguintes situações, os certificados podem ser revogados para o mesmo autor:

- quando a sua validade acaba expirando – os certificados apresentam validade previamente definida, depois da qual deixam de produzir os seus efeitos; e
- quando ocorre um problema de comprometimento de chaves – aqui, é necessário proceder com a invalidação.

Além disso, o certificado digital, após consumada a revogação, deve emitir listas de certificados invalidados, disponibilizando-as a toda comunidade de utilizadores. As organizações investem pesadamente na área de certificação digital, com o intuito de garantir autenticidade, confidencialidade e integridade às informações que circulam no ambiente web.

## 5.1 Requisitos das assinaturas digitais

Segundo Stallings (2015), é possível elencar alguns requisitos para as assinaturas digitais, dentre os quais podemos destacar os que se seguem.

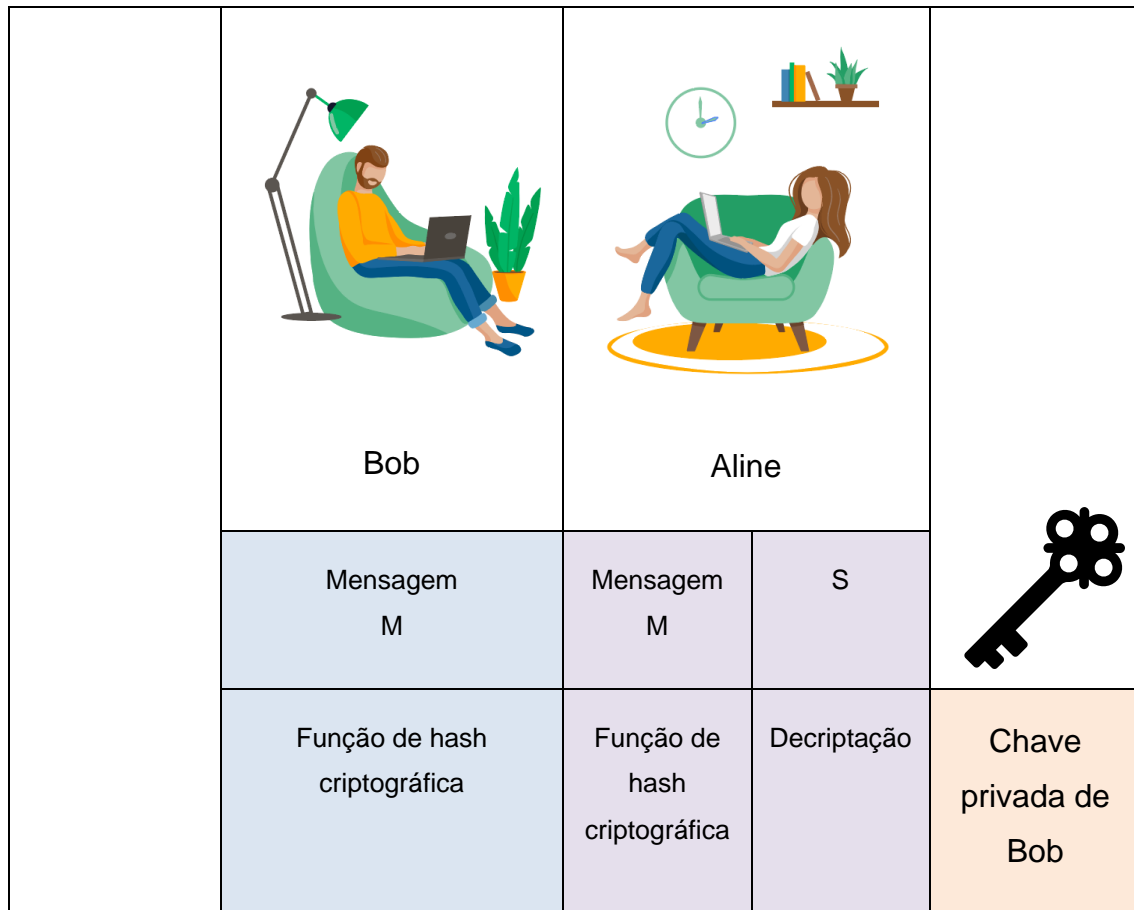
- A assinatura deve apresentar um padrão de bits que depende do fechamento e da assinatura da mensagem.




- A assinatura deve usar informações exclusivas do emissor, de modo a impedir a falsificação e a negação.
  - É preciso que a produção da assinatura digital seja relativamente fácil.
  - É preciso que o processo de reconhecer e verificar a assinatura digital seja relativamente fácil.
- É preciso que a falsificação computacional seja inviável, seja pela elaboração de uma nova mensagem para uma assinatura digital existente, ou por meio de uma assinatura digital fraudada para determinada mensagem.
- É preciso que a retenção de uma cópia de assinatura digital seja prática, em termos de armazenamento.

Uma função hash faz parte do processo de cifragem, oferecendo apoio para atingir alguns requisitos. A figura a seguir traz uma representação simplificada de alguns elementos essenciais ao processo de assinatura digital, com o exemplo de uma mensagem enviada de Bob para Alice.

Figura 9 – Elementos essenciais de assinatura digital





Chave privada de Bob	h	h	h'	
	Encriptação	Compara		
	S	Retorna assinatura válida ou não válida		
	Assinatura de Bob para M			

Fonte: Elaborado com base em Stallings, 2015.

A assinatura digital direta é um processamento que envolve apenas os atores da comunicação (emissor, receptor). Considera-se sempre que o receptor deve conhecer a chave pública de origem. A confidencialidade deve ser realizada para a etapa de encriptação da mensagem inteira, considerando ainda a assinatura de uma chave secreta (encriptação simétrica). A validade de processamento depende da segurança da chave privada do emissor. A certificação digital e as autoridades de certificação são técnicas universalmente aceitas para lidar com ameaças de segurança à assinatura digital.

## 5.2 Algoritmos de assinatura digital

Existem algoritmos de encriptação de mensagens por meio da chave pública de um usuário e de deciptação, utilizando a chave privada do mesmo usuário. Conforme apresentamos anteriormente, a assinatura digital com algoritmo de Elgamal utiliza números primos para a geração de pares de chaves (pública e privada). Já a assinatura digital usa o algoritmo Schnorr, com base em logaritmos discretos. O esquema de Schnorr minimiza a quantidade de cálculos necessários, e dependentes da mensagem, exigidos para a geração de uma assinatura. O processamento principal da geração de assinatura não depende exclusivamente da mensagem, de modo que ela pode ser executada com os tempos ociosos de processamento dos equipamentos.

O algoritmo de assinatura digital do NIST (National Institute of Standards and Technology) escolhido foi o algoritmo de assinatura digital (Digital Signature



Algorithm – DSA). O DSA utiliza funções hash (Secure Hash Algorithm – SHA), atendendo a anseios do público com relação à segurança em processos de assinatura digital. Esse esquema foi proposto em 1993. Na sequência, os algoritmos foram revistos, tendo sido incorporado ao esquema de assinatura digital o algoritmo RSA e o algoritmo de criptografia de curvas elípticas.

O DSA é um algoritmo que tem por base o cálculo de logaritmos discretos. Utiliza como referência os algoritmos de assinatura digital criados por Elgamal e Schnorr. Também utiliza número primos na criação de chaves. As fórmulas utilizadas para a criação e a verificação das chaves são mostradas na figura a seguir.

Figura 10 – Assinatura digital DSA

Componentes globais da chave pública $p$ número primo entre $2^{L-1} < p < 2^L$ para $512 \leq L \leq 1024$ e $L$ um múltiplo de 64; ou seja, o tamanho entre 512 e 1024 bits em incrementos de 64 bits. $q$ divisor primo $(p-1)$ , onde $2^{N-1} < q < 2^N$ , ou seja, tamanho $N$ bits $g = h(p-1)/q \bmod p$ , onde $h$ é qualquer inteiro em $1 < h < (p-1)$ , tal que $h(p-1)/q \bmod p > 1$	Assinatura $r = (gk \bmod p) \bmod q$ $s = [k^{-1} (H(M) + xr)] \bmod q$ Assinatura = $(r, s)$
Chave privada do usuário $x$ inteiro aleatório ou pseudoaleatório com $0 < x < q$	Verificação $W = (S)^{-1} \bmod q$ $U1 = [(H(M') w)] \bmod q$ $U2 = (r')w \bmod q$ $v = [(gu1 + yu2) \bmod p] \bmod q$  TESTE: $v = r'$
Chave pública do usuário $Y = gx \bmod p$	$M$ = mensagem a ser assinada $H(M)$ = hash de $M$ usando SHA-1
Número secreto por mensagem do usuário $K$ inteiro aleatório ou pseudoaleatório com $0 < k < q$	$M', r', s'$ = versões recebidas de $M, r, s$

Fonte: Elaborado com base em Stallings, 2015.

Outra técnica já mencionada é a assinatura digital baseada em criptografia de curva elíptica, chamada de Elliptic Curve Digital Signature



Algorithm (ECDSA). Essa técnica tem sido cada vez mais utilizada, por apresentar vantagens em termos de eficiência e segurança, mesmo com chaves menores que os demais métodos. O ECDSA apresenta as seguintes características.

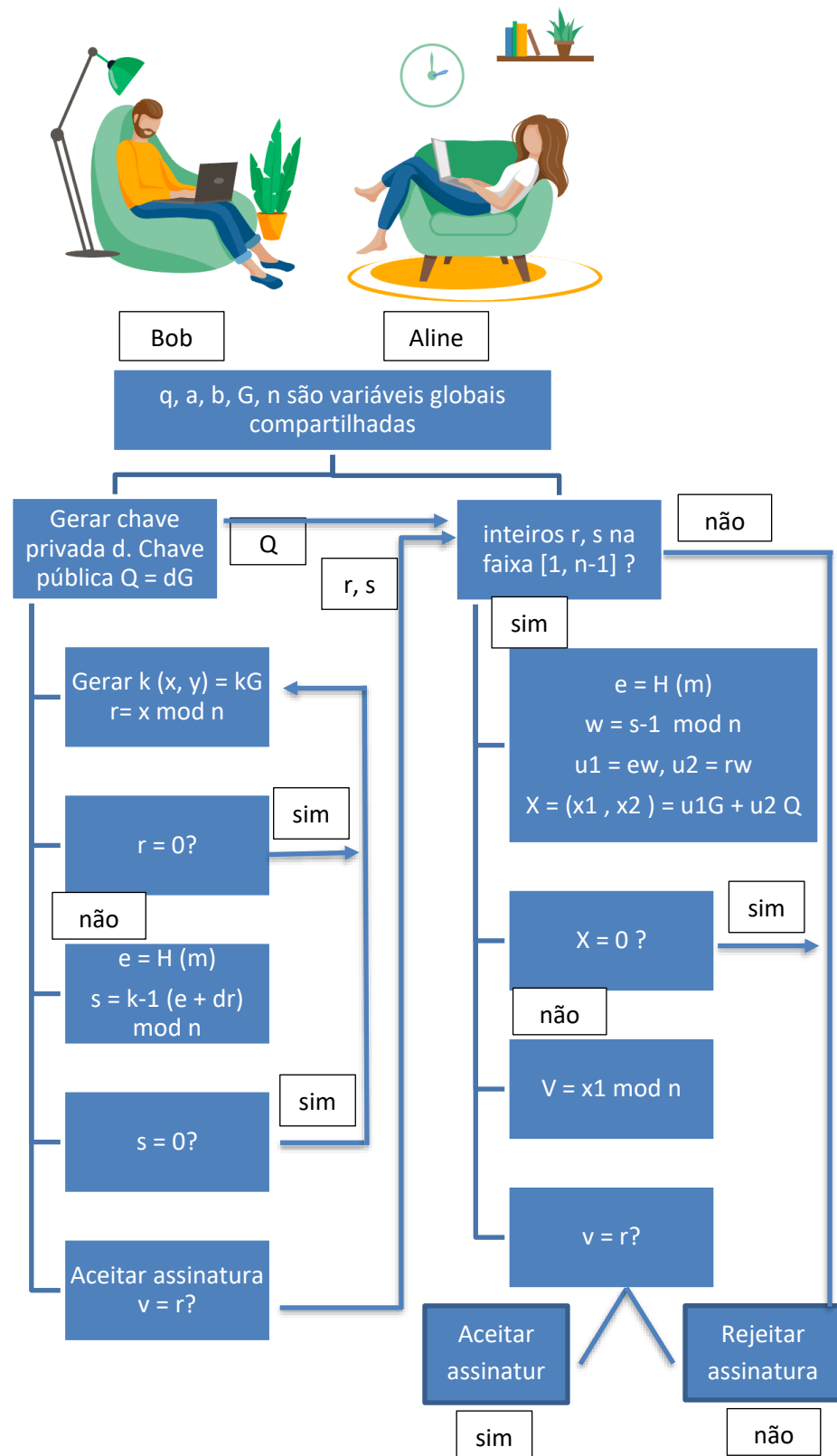
- Todos os participantes que utilizam o método de assinatura digital precisam usar os mesmos parâmetros de domínio global, com a definição de uma curva elíptica, gerando o ponto de origem na curva.
- Um utilizador, de início, precisa garantir a geração de seu par de chaves, tanto a pública quanto a privada. Para a criação de chave privada, o utilizador faz a seleção de um número aleatoriamente. Com esse valor e ponto de origem da curva, o utilizador, com a chave pública, calcula o outro ponto, formando a curva elíptica.
- Uma função hash gera um valor para que a mensagem seja assinada. Uma assinatura é criada combinando a chave privada, as configurações de domínio e o valor gerado pela função hash.
- Para os processos de verificação de assinaturas, a entrada é a chave pública do utilizador, as configurações de domínio e os valores gerados pela assinatura digital.

Em relação ao método operacional, o ECDSA apresenta as seguintes premissas.

- As assinaturas são exclusivas e nunca se repetem, para cada grupo de geração de chaves privadas e públicas.
- É impossível, em termos práticos, fazer qualquer tipo de falsificação de assinaturas digitais. Isso acontece porque os valores utilizados na potência computacional necessária para os cálculos estão bem fora dos limites atuais.

O ECDSA é considerado seguro por conta dessas premissas. Trata-se de um padrão largamente utilizado em infraestruturas de certificação digital (SSL e TLS). A criptomoeda Bitcoin também utiliza o algoritmo ECDSA em suas transações. A figura a seguir apresenta detalhes sobre o funcionamento do método ECDSA.

Figura 11 – Assinatura digital ECDSA



Fonte: Elaborado com base em Stallings, 2015.

### 5.3 Certificados X.509

A padronização X.509 apresenta boas práticas de serviços de diretório, que nada mais são do que um servidor, ou um grupo de servidores (sistema distribuído), que disponibilizam um banco de dados com todas as informações



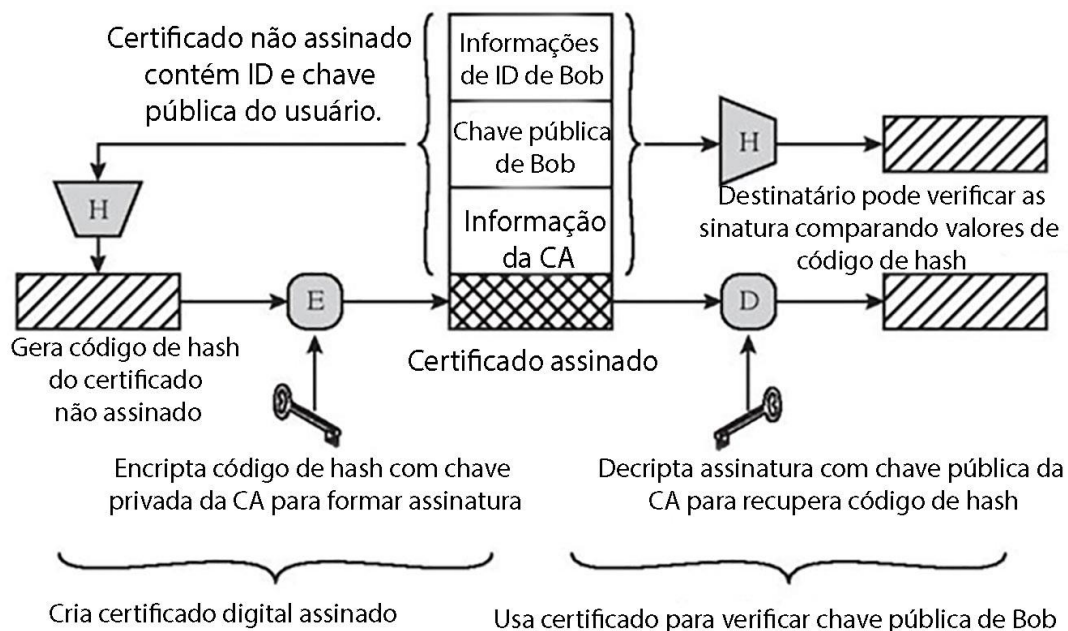


dos usuários. Dentro desse banco de dados, existem informações relacionadas com nomes de usuários e endereçamentos de rede, entre outros dados, atributos e detalhes dos usuários.

Dentro do X.509, há uma estrutura de provisionamento de serviços de autenticação, que usa como base o diretório dos seus usuários. Dentro do repositório de certificados, ficam as chaves públicas. Cada chave pública de usuário apresenta um certificado assinado com a chave privada de uma Autoridade Certificadora confiável. Existem também, dentro dessa estrutura, protocolos relacionados com a autenticação de usuários para a utilização dos certificados. Esse padrão foi proposto em 1988. Por conta de falhas de segurança, foi revisado em 1993. Uma terceira versão foi lançada em 2000.

O X.509 foi criado e desenvolvido com base em criptografia de chave pública e assinaturas digitais. Não há um algoritmo específico, mas o padrão recomendado é o RSA. Uma função hash é necessária para a checagem. A figura a seguir ilustra o processo da geração de um certificado digital de chave pública.

Figura 12 – Geração de certificado digital



Fonte: Elaborado com base em Stallings, 2015.

No Brasil, foi adotada a ICP-Brasil<sup>7</sup>, uma tecnologia de certificação digital com infraestrutura de chaves públicas no formato hierárquico, de maneira bem centralizada, vinculada ao Governo Federal. A ICP-Brasil não está interligada



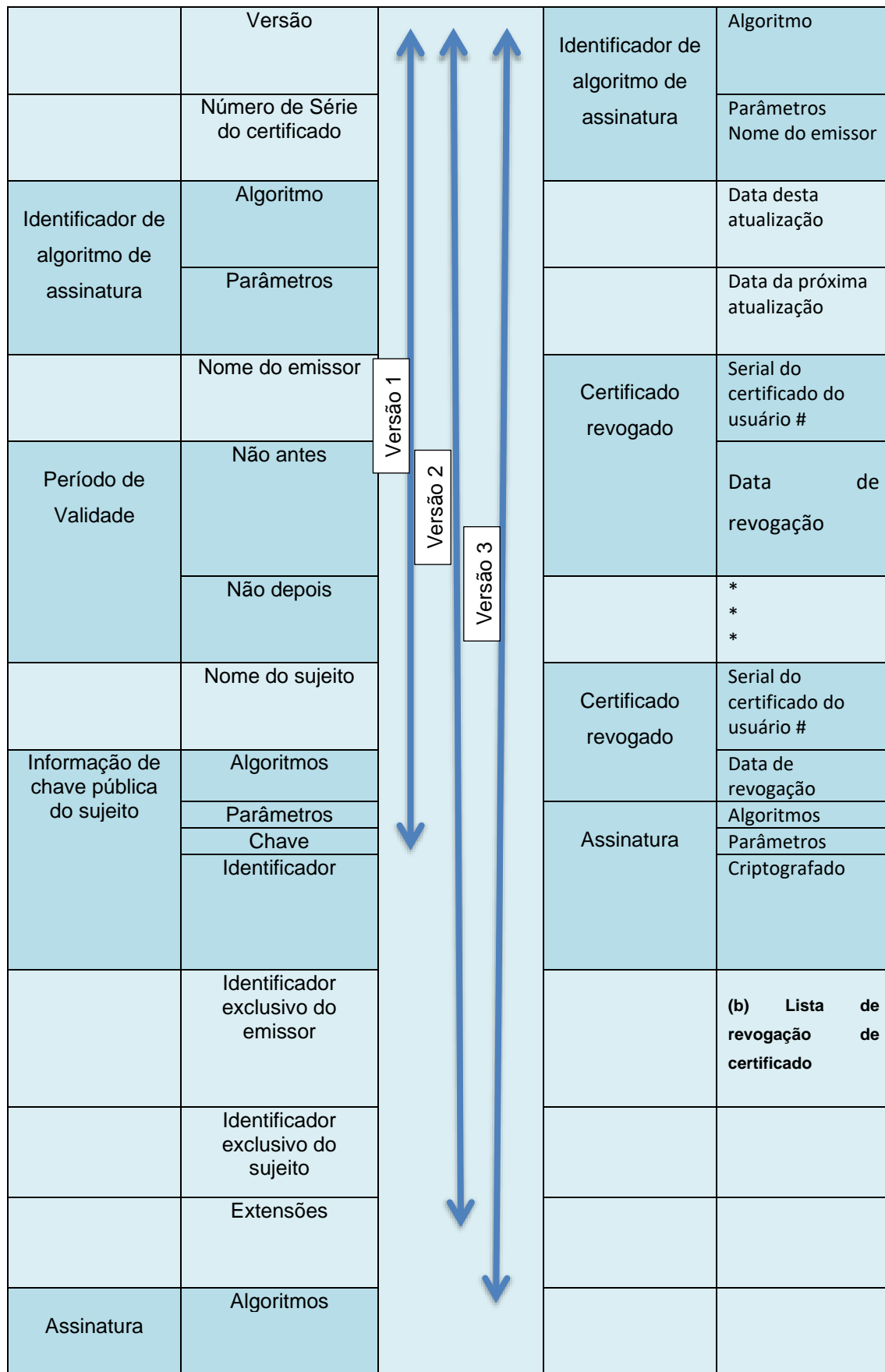
apenas ao âmbito da administração pública, por mais que esteja vinculada ao contexto de política de segurança, publicação e divulgação da informação. Ela também ingressou na iniciativa privada, com o intuito de minimizar a insegurança jurídica geral, com papel de destaque na validade de documentos eletrônicos.

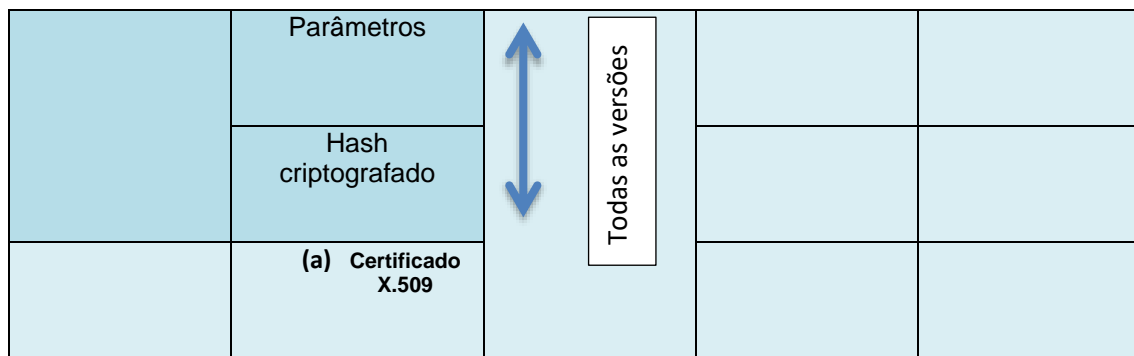
A Autoridade Certificadora Raiz da ICP-Brasil é o Instituto Nacional de Tecnologia da Informação (ITI), autarquia pertencente à administração pública federal, ligado à Casa Civil da Presidência da República.

Os certificados digitais de usuários são criados e gerenciados por uma Autoridade Certificadora confiável, sendo armazenados dentro dos diretórios da CA ou pelo próprio usuário. O formato e a estrutura geral de um certificado está representado, com todos os seus elementos, na figura a seguir.



Figura 13 – Formato do Certificado X.509





Fonte: Elaborado com base em Stallings, 2015.

## FINALIZANDO

Nesta aula, apresentamos alguns frameworks de gestão de apoio à segurança da informação, com destaque para o CIS Controls e o NIST CSF, referências de mercado, sendo comumente utilizados pelos americanos. Posteriormente, abordamos a criptografia e suas técnicas; a história e a origem da criptografia; as funções hash, que garantem a integridade e a checagem de dados; as assinaturas digitais; a certificação digital; além dos algoritmos de criptografia simétrica e assimétrica. O objetivo desta aula foi descrever os principais mecanismos que garantem a segurança no transporte de informações, com a consequente integridade e veracidade das informações para os utilizadores da internet.



## REFERÊNCIAS

ALVES, D. **Internet das Coisas (IoT):** segurança e privacidade de dados pessoais Rio de Janeiro: Alta Books, 2021.

FRAGA, B. **Técnicas de invasão:** aprenda as técnicas usadas por hackers em invasões reais São Paulo: Labrador, 2019.

NIST – Nist Cybersecurity Framework. An Introduction to the Components of the Framework. **Cybersecurity Framework**, 6 fev. 2018. Disponível em: <<https://www.nist.gov/cyberframework/online-learning/components-framework>>. Acesso em: 24 jan. 2022.

STALLINGS, W. **Criptografia e segurança de redes princípios e práticas.** 6. ed. São Paulo: Pearson Education do Brasil, 2015.