



**APOSTILA** DIGITAL

Nível:  
**Superior**



EDIÇÃO **2024**

FORMATO **[PDF]**

## Quem Somos

A Domina Concursos, especialista no desenvolvimento e comercialização de apostilas digitais e impressas para Concurso Públicos, tem como foco tornar simples e eficaz a forma de estudo. Com visão de futuro, agilidade e dinamismo em inovações, se consolida com reconhecimento no segmento de desenvolvimento de materiais para concursos públicos. É uma empresa comprometida com o bem-estar do cliente. Atua com concursos públicos federais, estaduais e municipais. Em nossa trajetória, já comercializamos milhares de apostilas, sendo digitais e impressas. E esse número continua aumentando.

## MISSÃO

Otimizar a forma de estudo, provendo apostilas de excelência, baseados nas informações de editais dos concursos públicos, para incorporar as melhores práticas, com soluções inovadoras, flexíveis e de simples utilização e entendimento.

## VISÃO

Ser uma empresa de Classe Nacional em Desenvolvimento de Apostilas para Concursos Públicos, com paixão e garra em tudo que fazemos.

## VALORES

- Respeito ao talento humano
- Foco no cliente
- Integridade no relacionamento
- Equipe comprometida
- Evolução tecnológica permanente
- Ambiente diferenciado
- Responsabilidade social



HABILITADA P/ IMPRESSÃO



## PROIBIDO CÓPIA

Não é permitida a revenda, rateio, cópia total ou parcial sem autorização da Domina Concursos, seja ela cópia virtual ou impressa. Independente de manter os créditos ou não, não importando o meio pelo qual seja disponibilizado: link de download, Correios, etc...

Caso houver descumprimento, o autor do fato poderá ser indiciado conforme art. 184 do CP, serão buscadas as informações do responsável em nosso banco de dados e repassadas para as autoridades responsáveis.







★★★★★  
NOVA DIDÁTICA

CONCURSOS

**DOMINA**  
CONCURSOS

→ **Conhecimento  
Específico**



EDIÇÃO **2024**

FORMATO **[PDF]**



## Segurança em Banco de dados: Integridade de dados

A principal característica de um sistema é controlar os processos de uma empresa. Dessa forma, cada solução que encontramos hoje no mercado de tecnologia possui características com objetivo de proporcionar aos clientes uma qualidade considerável em requisitos de segurança, performance, escalabilidade e, acima de tudo, coerência no uso da informação.

Esta coerência se trata de garantir que uma informação será verdadeira, será confiável e íntegra.

Quando um sistema controla os dados de uma organização, estes dados devem ser cuidadosamente analisados, afinal eles estarão de alguma forma interligados entre si no que diz respeito ao processo do negócio como um todo.

Por exemplo, um cadastro de fornecedores estará de alguma forma se comunicando com o cadastro de produtos, afinal os produtos pertencem a um fornecedor. Assim, a integridade de uma entidade pode ter impacto diretamente em outra entidade.

Normalmente cada funcionário tem um cargo e uma função; operar um sistema faz parte do dia a dia deste funcionário. Quando existe mais de um funcionário com a mesma função, eles utilizam o mesmo sistema e realizam os mesmos processos.

Isso pode parecer simples, porém se um sistema não tiver regras de integridade de dados, a forma de inserir os dados neste sistema ocorrerá de forma desordenada, causando um grande problema de registros sem uma regra definida ou mesmo inseridos de forma incorreta.

Podemos imaginar agora um ambiente de uma empresa que usa um sistema para controlar seus processos e, em um determinado momento, optam por criar um BI. Quando criamos um BI, partimos do princípio de que existe uma integridade na informação que será inserida neste BI.

Toda informação do sistema que controla a empresa será enviado por algum processo de ETL para esse BI. Um sistema sem integridade de dados pode resultar em um BI não confiável e com uma informação falsa.

### BOX 1. ETL

O Extract Transform Load dá nome às ferramentas que têm como função a extração de dados em diversos sistemas, fazem tratamentos e transformações nestes dados, para então inseri-los em DataWarehouses e Data Marts.

Geralmente este BI é consultado por diretores das empresas para apoiarem na tomada de decisões em várias esferas do negócio, e pode funcionar como um termômetro para medir se, por exemplo, um produto é viável ou não no mercado.

Podemos perceber que a falta de integridade na informação pode trazer danos irreversíveis para o negócio, podendo causar problemas de impactos financeiros.

Analistas, desenvolvedores, ADs e DBAs, consomem uma boa parte de seu tempo planejando como usar as regras de integridade de dados nos SGBDs de forma eficiente. Visando esta necessidade, demonstraremos neste artigo os mecanismos existentes para garantir a integridade da informação, e demonstraremos em exemplos práticos como implementar as regras no SQL Server e no Oracle.

## Segurança em Banco de Dados: conheça as 5 principais causas de ataques

Atualmente, o maior bem que uma empresa possui é a informação. E, quando se trata de manter a confiabilidade dos próprios dados, são muitos os desafios enfrentados — sendo a segurança em banco de dados um dos maiores deles.

Por várias perspectivas, existem ameaças à integridade da informação que transita dentro de uma organização. Cabe, então, aos especialistas contratados moderar a ocorrência desse cenário e agir de forma concisa contra investidas não autorizadas.

Nesse sentido, é muito importante ter conhecimento sobre as principais brechas possíveis que podem existir nos bancos de dados empresariais. Por isso, continue lendo e veja as principais causas de ataques para que você se previna e não permita que isso aconteça na sua empresa!

## 5 principais causas de ataques a banco de dados

### 1. SQL Injection

O tipo mais conhecido de ataque a banco de dados é o SQL Injection. Nessa possibilidade, são incluídas instruções não autorizadas e mal-intencionadas no sistema, que podem dar os mais diversos privilégios ao agente invasor.

Um hacker que consegue acesso usando SQL Injection pode dar a si mesmo permissão total de manipulação das informações armazenadas, e causar um enorme estrago nos dados mal protegidos da empresa.

Existe ainda uma segunda categoria de ataques de injeção: o NoSQL Injection, que age em cima de soluções Big Data.

Assim, para que essas aberturas a acessos indevidos não aconteçam, os bancos devem estar muito bem codificados, com a segurança sempre em dia. A natureza dessas soluções já não utiliza nenhum comando SQL, impossibilitando o primeiro tipo de ataque.

### 2. Privilégios demais a pessoas demais

Controlar o que se pode acessar e quais ações podem ser realizadas em cima das informações é uma parte básica da segurança em banco de dados. Contudo, existem empresas que ainda não se preocupam com esse risco.

Se muitas pessoas têm acessos a dados sensíveis ou ao ambiente de produção, por exemplo, é muito possível — mesmo que de forma não intencional — que um colaborador delete informações que vão parar o funcionamento de vários sistemas.

E isso pode acarretar em um prejuízo financeiro de forma imediata a empresa. Além do problema do dinheiro, o tempo que será gasto pelo DBA para “apagar esse incêndio” será outro prejuízo em grande escala.

Afinal, uma situação dessas atrasa todos os outros projetos evolutivos em andamento, impedindo a empresa de crescer por uma total falta de cuidado com seu ativo mais precioso.

### 3. Deficiência na auditoria

Quando novas tabelas, ou mesmo campos são criados em um banco de dados, eles devem passar por um processo extremamente rigoroso de auditoria. Não se pode deixar passar nada, pois um simples erro, como um caractere a menos em um campo, já pode parar o sistema de forma geral.

E como ninguém deveria poder alterar um banco em horários não planejados, isso pode fazer com que durante o restante do dia os funcionários não possam trabalhar mais nos sistemas que acessam o banco de dados.

Caso a empresa não possua recursos ou conhecimento suficiente para garantir a integridade do banco de dados, é interessante terceirizar esse serviço, deixando que profissionais especializados cuidem da saúde do sistema e impedindo que cenários de bloqueio do trabalho de outras áreas **ocorra**.

### 4. Sistemas de segurança fracos e/ou desatualizados

Um erro muito comum que os usuários cometem nas empresas é ter senhas fáceis, ou até manter as senhas padrão em seu acesso. E, a partir de uma falha como essas, todos podem sair perdendo.

A importância de fortificar a senha deve ser muito bem esclarecida a todos, mesmo aos que não possuem conhecimentos de segurança.

Nesse sentido, os firewalls e as políticas de bloqueio e exceção devem ser sempre atualizadas, e técnicos com alta capacidade devem ser mantidos para cuidar dessa atividade. Até porque nenhum sistema é completamente livre de invasões.

Tecnologias que já estão ultrapassadas, com certeza, já foram destrinchadas por hackers e são mais vulneráveis a quem possui esse tipo de conhecimento.

Justamente por isso, são lançadas, periodicamente, novas versões de programas de proteção, que buscam estar sempre à frente de ataques — e esse ciclo continuará. Logo, para manter seguros seus dados, é preciso usar programas confiáveis, pessoas competentes e manter as atualizações em dia.

## **5. Exposição de mídia storage**

Muitos casos de ataques também ocorrem a backups mal protegidos, e não à base principal de uma corporação. Por isso, quando são feitos backups do banco de dados, é extremamente importante lembrar que a segurança da mídia storage deve ser, pelo menos, igual à do servidor original.

Inclusive, o cuidado com essa tarefa deve ser o mesmo, pois faz parte de atividades que sempre serão realizadas. Assim, uma boa solução é realizar os backups na nuvem, pois a segurança nesse ambiente está sempre à frente em termos de novas tecnologias.

Caso sejam escolhidos backups locais, o processo a seguir deve ser definido e auditado, pois uma cópia da base mal protegida já é uma porta de entrada para quem quer prejudicar sua empresa.

### **Como cuidar da segurança em banco de dados da sua empresa**

É trabalho dos responsáveis pela empresa zelar pela segurança das informações que pertencem a ela. E, para realizar isso com sucesso, é essencial ter um time de alta competência — seja ele próprio ou terceirizado.

Ter conhecimento sobre as tecnologias que garantem maior segurança e saber que isso tem um custo a arcar são atitudes que dão aos gerentes e líderes mais confiança para garantir a integridade dos dados.

Além disso, é sempre importante lembrar, os gastos com a proteção do banco de dados, com certeza, serão menores que os prejuízos de uma invasão, um roubo ou um vazamento de informações cruciais para o negócio.

O armazenamento acaba se tornando parte fundamental do corpo de uma empresa, pois registrar todo o histórico do negócio é fundamental para seus planos futuros. Por isso, investir na segurança em banco de dados é parte essencial do crescimento empresarial saudável e da busca por se destacar no mercado!

E aí, gostou do post? Essas dicas sobre como proteger seu banco de dados foram úteis? Então, aproveite agora para assinar a nossa newsletter e continue por dentro de muitos outros assuntos do mundo da tecnologia!

### **Conceitos sobre Segurança em Banco de Dados**

Os bancos de dados são utilizados para armazenar diversos tipos de informações, desde dados sobre uma conta de e-mail até dados importantes da Receita Federal. A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade. Um Sistema gerenciador de banco de dados deve fornecer mecanismos que auxiliem nesta tarefa.

Os bancos de dados SQL implementam mecanismos que restringem ou permitem acessos aos dados de acordo com papéis ou roles fornecidos pelo administrador. O comando GRANT concede privilégios específicos para um objeto (tabela, visão, seqüência, banco de dados, função, linguagem procedural, esquema ou espaço de tabelas) para um ou mais usuários ou grupos de usuários.

A preocupação com a criação e manutenção de ambientes seguros se tornou a ocupação principal de administradores de redes, de sistemas operacionais e de bancos de dados. Pesquisas mostram que a maioria dos ataques, roubos de informações e acessos não- autorizados são feitos por pessoas que pertencentes à organização alvo.

Por esse motivo, esses profissionais se esforçam tanto para criar e usar artifícios com a finalidade de eliminar os acessos não-autorizados ou diminuir as chances de sucesso das tentativas de invasão (internas ou externas). Os controles de acesso em sistemas de informação devem certificar que todos os acessos diretos ao sistema ocorram exclusivamente de acordo com as modalidades e as regras pré-estabelecidas, e observadas por políticas de proteção.

De modo geral, os mecanismos de segurança referem-se às regras impostas pelo subsistema de segurança do SGBD, que verifica todas as solicitações de acesso, comparando-as com as restrições de segurança armazenadas no catálogo do sistema. Entretanto existem brechas no sistema e ameaças externas que podem resultar em um servidor de banco de dados comprometido ou na possibilidade de destruição ou no roubo de dados confidenciais.

As ameaças aos bancos de dados podem resultar na perda ou degradação de alguns ou de todos os objetivos de segurança aceitos, são eles: integridade, disponibilidade, confidencialidade. A integridade do banco de dados se refere ao requisito de que a informação seja protegida contra modificação imprópria.

A disponibilidade do banco de dados refere-se a tornar os objetos disponíveis a um usuário ou a um programa ao qual eles têm um direito legítimo. A confidencialidade do banco de dados se refere à proteção dos dados contra a exposição não autorizada. O impacto da exposição não autorizada de informações confidenciais pode resultar em perda de confiança pública, constrangimento ou ação legal contra a organização.

### **Controle de Acesso**

É todo controle feito quanto ao acesso ao BD, impondo regras de restrição, através das contas dos usuários. O Administrador do BD (DBA) é o responsável superior por declarar as regras dentro do SGBD. Ele é o responsável por conceder ou remover privilégios, criar ou excluir usuários, e atribuição de um nível de segurança aos usuários do sistema, de acordo com a política da empresa.

### **Controle de Inferência**

É um mecanismo de segurança para banco de dados estatísticos que atua protegendo informações estatísticas de um indivíduo ou de um grupo. Bancos de dados estatísticos são usados principalmente para produzir estatísticas sobre várias populações.

O banco de dados pode conter informações confidenciais sobre indivíduos. Os usuários têm permissão apenas para recuperar informações estatísticas sobre populações e não para recuperar dados individuais, como, por exemplo, a renda de uma pessoa específica.

### **Controle de Fluxo**

É um mecanismo que previne que as informações fluam por canais secretos e violem a política de segurança ao alcançarem usuários não autorizados. Ele regula a distribuição ou fluxo de informação entre objetos acessíveis. Um fluxo entre o objeto A e o objeto B ocorre quando um programa lê valores de A e escreve valores em B. Os controles de fluxo têm a finalidade de verificar se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção. Dessa maneira, um usuário não pode obter indiretamente em B aquilo que ele ou ela não puder obter diretamente de A.

### **Criptografia de Dados**

Você pode ler aqui um pouco mais sobre criptografia. É uma medida de controle final, utilizada para proteger dados sigilosos que são transmitidos por meio de algum tipo de rede de comunicação. Ela também pode ser usada para oferecer proteção adicional para que partes confidenciais de um banco de dados não sejam acessadas por usuários não autorizados. Para isso, os dados são codificados através da utilização de algum algoritmo de codificação. Assim, um usuário não autorizado terá dificuldade para decifrá-los, mas os usuários autorizados receberão chaves para decifrar esses dados. A criptografia permite o disfarçada mensagem para que, mesmo com o desvio da transmissão, a mensagem não seja revelada.

### **Usuários**

Abrange usuários e esquema do banco de dados onde cada banco de dados Oracle tem uma lista de nomes de usuários. Para acessar um banco de dados, um usuário deve usar um aplicativo desse tipo e tentar uma conexão com um nome de usuário válido. Cada nome tem uma senha associada para evitar o uso sem autorização.

Devem ser implementados ainda diferentes perfis de usuário para diferentes tarefas no Oracle, tendo em vista que cada aplicação/usuário tem a sua necessidade de acesso. Existe ainda a possibilidade de proteger os perfis com senha, o que é uma excelente medida. Além dessas medidas, o uso de cotas aumenta a restrição de espaço em disco a ser utilizado por usuários/aplicativos.



## Domínio de Segurança

Onde cada usuário tem um domínio de segurança, um conjunto de propriedades que determinam coisas como ações (privilegios e papeis) disponíveis para o usuário; cota de tablespaces (espaço disponível em disco) do usuário; limites de recursos de sistema do usuário.

As tabelas (tablespaces) do sistema, como a system, devem ser protegidas de acessos de usuários diferentes dos usuários de sistema. A liberação de escrita e alteração de dados em tais tabelas é muito comum em ambientes de teste, onde os programadores e DBAs tomam tal atitude para evitar erros de aplicação por falta de privilégios. Porém, em ambientes de produção, tal medida é totalmente desaconselhável.

## Autoridade

As autoridades fornecem um método de agrupar privilégios e controlar o nível de acesso dos administradores e operadores da base de dados com relação à manutenção e operações permitidas. As especificações da base de dados estão armazenadas em catálogos da própria base de dados. As autoridades do sistema estão associadas a membros de grupos e armazenados no arquivo de configuração administrativa do banco de dados. Este arquivo define as concessões de acesso e o que poderá ser executado de acordo com cada grupo.

## Privilégios

Os privilégios são permissões únicas dadas a cada usuário ou grupo. Eles definem permissões para tipos de autorização. Pelos privilégios é possível autorizar o usuário a modificar ou alcançar determinado recurso do Banco de Dados.

Os privilégios também são armazenados em catálogos do próprio Banco de Dados, visto que os grupos de autoridade por já possuírem grupos predefinidos de privilégio concedem implicitamente privilégios a seus membros.

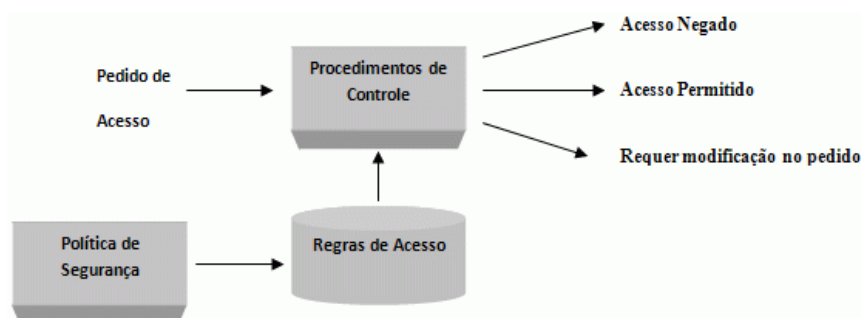
## Tipos de privilégios discricionários

O SGBD deve oferecer acesso seletivo a cada relação do banco de dados baseando-se em contas específicas. As operações também podem ser controladas; assim, possuir uma conta não necessariamente habilita o possuidor a todas as funcionalidades oferecidas pelo SGBD. Informalmente existem dois níveis para a atribuição de privilégios para o uso do sistema de banco de dados:

- O nível de conta: Nesse nível, o DBA estabelece os privilégios específicos que cada conta tem, independente das relações no banco de dados.
- O nível de relação (ou tabela): Nesse nível, o DBA pode controlar o privilégio para acessar cada relação ou visão individual no banco de dados.

## Revogação de Privilégios

Em alguns casos, interessa conceder um privilégio temporário a um usuário. Por exemplo, o proprietário de uma relação pode querer conceder o privilégio SELECT a um usuário para uma tarefa específica e depois revogar aquele privilégio quando a tarefa estiver completada. Por isso, é necessário um mecanismo para a revogação de privilégios. Em SQL, um comando REVOKE é introduzido com o intento de cancelar privilégios.



## Sistema de Controle de Acesso

### Controle de acesso obrigatório e para segurança multi-nível

Neste método, o usuário não tem um meio termo, ou ele tem ou não tem privilégios, sendo utilizado normalmente em BD que classificam dados de usuários, onde é necessário um nível a mais de segurança. A maioria dos SGBDs não oferecem esse tipo de controle de acesso obrigatório, ficando com os controles discricionários ditos anteriormente. Normalmente são utilizados em sistemas governamentais, militares ou de inteligência, assim como industriais e corporativas.

As **classes de segurança** típicas são altamente sigilosas (top secret, TS), secreta (secret, S), confidenciais (confidential) (C) e não Classificada (unclassified, U), em que TS é o nível mais alto e U é o mais baixo.

De uma forma geral, os mecanismos de controle de acesso obrigatório impõem segurança multinível, pois exigem a classificação de usuários e de valores de dados em classes de segurança e impõem as regras que proíbem o fluxo de informação a partir dos níveis de segurança mais altos para os mais baixos.

### Controle de acesso baseado em papéis

É uma abordagem para restringir o acesso a usuários autorizados e uma alternativa aos sistemas de controles de acesso do tipo MAC e DAC. O conceito de controle de acesso baseado em papéis surgiu com os primeiros sistemas computacionais multiusuários interativos. A ideia central do RBAC é que permissões de acesso são associadas a papéis, e estes papéis são associados a usuários. Papéis são criados de acordo com os diferentes cargos em uma organização, e os usuários são associados a papéis de acordo com as suas responsabilidades e qualificações. Vários indivíduos podem ser designados para cada papel. Os privilégios de segurança comuns a um papel são concedidos ao nome dele, e qualquer indivíduo designado para esse papel automaticamente teria esses privilégios concedidos.

Os usuários podem ser facilmente remanejados de um papel para outro. Mudanças no ambiente computacional, como instalação de novos sistemas e remoção de aplicações antigas, modificam apenas o conjunto de permissões atribuídas aos diferentes papéis, sem envolver diretamente o conjunto de usuários.

A separação de tarefas é um requisito importante em diversos SGBDs. É necessária para impedir que um usuário realize sozinho o trabalho que requer o envolvimento de outras pessoas. A exclusão mútua de papéis é um método que pode ser implementado com sucesso.

Outro aspecto relevante nos sistemas RBAC são as restrições temporais possíveis que podem existir nos papéis, como o tempo e a duração das ativações de papéis e o disparo temporizado de um papel por uma ativação de outro papel. O uso de um modelo RBAC é um objetivo altamente desejado para solucionar os principais requisitos de segurança das aplicações baseadas na web.

### Controle de acesso utilizando Triggers

Com a utilização das Triggers é possível criar mecanismos de segurança mais complexos que podem ser disparados cada vez que um evento é chamado. O comando Insert na tabela é exemplo de um evento que pode ser usado para disparar uma Triggers, além disso, as mesmas podem ser disparadas antes ou depois de comando especificado com o objetivo de prover maior rigor no controle de segurança.

Se o comando executado pelo usuário não for validado pela Triggers, um erro é sinalizado do corpo da própria Triggers para impedir que a tabela seja modificada indevidamente.

### Controle de acesso utilizando Views

As views constituem um outro método de controle de acesso, normalmente utilizadas para restringir o acesso direto aos dados. Com a view é possível permitir acesso de usuário concedendo privilégios, ocultar linhas e colunas de informações confidenciais ou restritas residentes na tabela original das indicações do SQL.

Os privilégios e concessões são definidos somente na view e não afetam a tabela base sendo o acesso dos usuários delimitado pela view, a qual é gerada criando um subconjunto de dados na tabela referenciada.

## Políticas de Acesso aos Documentos de Arquivo

Políticas públicas de arquivo, política institucional de arquivos e gestão de documentos são dimensões que interessam ao universo da Arquivologia e que podem ser desenvolvidas de maneira independente. Contudo, é fortemente recomendável que haja ampla interlocução entre elas, para assegurar o sucesso das propostas e a perenidade dos resultados. O contrário disso implica prejuízos para os objetivos que cada uma propõe. Ao tratar de documentos públicos, a articulação dessas dimensões não pode desprezar a legislação arquivística como elemento balizador e que deve ser referência de qualquer diretriz, proposta, programa, projeto, ação ou procedimento que se cogite elaborar ou realizar.

### Políticas públicas de arquivos, política institucional de arquivo, legislação arquivística

Políticas públicas compreendem ações, metas e planos que os governos, nos âmbitos nacional, estadual e municipal, delineiam visando ao bem-estar da sociedade e ao interesse público. Todavia, a construção de uma política pública e sua implementação não dependem apenas do Poder Público, devendo contar também com o envolvimento de outros atores e da sociedade como um todo. Não se trata, portanto, apenas de um conjunto de decisões. “Uma política pública é concebida, formulada e implementada a partir de personagens que se relacionam, que se influenciam mutuamente, em um ambiente de conflitos e consensos” (SILVA, 2008, p. 3). Saliente-se, ainda, que legislação não é sinônimo de política pública, embora os dispositivos legais possam representar marcos importantes em sua construção, propulsionando-a. Saravia (2006) entende que política pública é...

[...] um fluxo de decisões públicas, orientado a manter o equilíbrio social ou a introduzir desequilíbrios destinados a modificar essa realidade. Decisões condicionadas pelo próprio fluxo e pelas reações e modificações que elas provocam no tecido social, bem como pelos valores, ideias e visões dos que adotam ou influem na decisão. É possível considerá-las como estratégias que apontam para diversos fins, todos eles, de alguma forma, desejados pelos diversos grupos que participam do processo decisório.

[...] Com uma perspectiva mais operacional, poderíamos dizer que ela é um sistema de decisões públicas que visa a ações ou omissões, preventivas ou corretivas, destinadas a manter ou modificar a realidade de um ou vários setores da vida social, por meio da definição de objetivos e estratégias de atuação e da alocação dos recursos necessários para atingir os objetivos estabelecidos (SARAVIA, 2006, p. 28-29, grifo nosso).

Saravia ainda declara que a finalidade última de tal dinâmica (consolidação da democracia, justiça social, manutenção do poder e felicidade das pessoas) é orientar as inúmeras ações que compõem determinada política. Neste sentido, “as políticas públicas funcionam como instrumento de aglutinação de interesses em torno de objetivos comuns, que passam a estruturar uma coletividade de interesses” (SOUZA, 2006, p. 3). Também destacando aspectos sociais da política pública, Silva afirma:

Ao conceituarmos ‘políticas públicas’, notamos a noção de que as decisões devem ser viabilizadas ante as necessidades coletivas. Caracterizam-se como ações do governo para os governados, no combate das diferenças e das desigualdades da vida social, por meio de decisões coletivas através de instituições administrativas do Estado, configuradas como ações que visam o bem estar comum. Quando acontece a intervenção estatal na vida social, verificamos a implementação da política pública (SILVA, 2013, p. 47).

Alguns problemas entram na agenda governamental como alvo de uma política pública; outros, não. A princípio, pode-se imaginar que a causa prende-se à limitação de recursos (econômicos e humanos), mas pode se dar também em virtude da falta de legislação ou de vontade política e de pouca “pressão” dos meios de comunicação ou dos setores envolvidos (SUBIRATS, 2006). Uma política pública despertará mais sensibilidade e, por conseguinte, maior mobilização a depender da relevância do tema, questão ou problema em foco. Mas, pergunta-se: Quais fatores ou circunstâncias conferem importância a determinado tema, questão ou problema para que sejam contemplados em um projeto, programa ou política pública? Recorre-se novamente a Subirats para tentar responder à questão. O autor avalia que um problema pode de fato ser um “problema público” e entrar na agenda governamental:

a) Se o tema ou questão atingiu proporções de “crise” e, portanto, não pode continuar a ser ignorado. [...] Outra possibilidade é que o tema apresente claras possibilidades de agravamento no futuro, com o que se pretende antecipar uma previsível situação de crise;

- b) quando adquiriu características peculiares ou significativas que o diferenciam de uma problemática mais geral;
- c) quando o problema causa uma situação emocional grave, que atrai atenção da mídia;
- d) quando um tema adquire importância global, mas em seu início tinha dimensões e efeitos muito limitados;
- e) temas que desencadeiam questões relacionadas à "legitimidade" ou "poder" e que, portanto, afetam o núcleo sensível do poder público, arrastando uma grande carga simbólica;
- f) questões que alcançam grande notoriedade pública, por se conectarem com tendências ou valores mais em voga (SUBIRATS, 2006, p. 205-206, tradução nossa).

Um problema relevante é central na formulação de uma boa política pública, mas não basta per se. “Uma política pública de qualidade incluirá diretrizes ou conteúdo, instrumentos ou mecanismos, definições ou modificações institucionais e a previsão de seus resultados” (LAHERA PARADA, 2006, p. 69, tradução nossa). Uma política pública de excelência corresponde à relação entre os cursos de ação e os fluxos de informação, com um objetivo político definido de maneira democrática e com o envolvimento dos setores público e privado e da comunidade, caracterizando-se por:

1. fundamentação ampla, e não apenas específica;
2. estimativa de custos e alternativas de financiamento;
3. fatores para uma avaliação social de custo-benefício;
4. benefício social secundário comparado a outras políticas;
5. consistência interna e agregada;
6. apoios e críticas prováveis (políticas, corporativas e acadêmicas);
7. oportunidade política;
8. sequência de medidas relevantes (O que vem primeiro? O que condiciona o quê?);
9. clareza dos objetivos;
10. funcionalidade dos instrumentos;
11. indicadores (custo unitário, economia, eficácia e eficiência) (LAHERA PARADA, 2006, p. 70, tradução nossa).

Pressupõe-se que, para elaborar uma política pública, é necessária uma visão holística, para melhor compreensão do contexto em que está inserida. Em se tratando de arquivos, esse contexto é o informacional. Dessa forma, políticas públicas de arquivo estão contidas no bojo das políticas públicas de informação. A noção de “política de informação”, de acordo com Jardim (2003, p. 40), tem a tendência de ser “naturalizada e a designar diversas ações e processos do campo informacional: arquivos, bibliotecas, internet, tecnologia da informação, governo eletrônico, sociedade da informação, informação científica e tecnológica, etc”. Uma política de informação não se caracteriza por ser um conjunto de decisões governamentais. Para constituí-la, é mister definir os universos geográfico, administrativo, econômico, temático, social e informacional, bem como prever os diversos atores do Estado e da sociedade que podem atuar em sua elaboração, implantação, controle e avaliação.

Quanto às políticas públicas de arquivo, seus objetivos “devem ser pautados, inicialmente, pelo direito do cidadão à informação e, também, pelo apoio à administração, à proteção da memória e ao desenvolvimento científico” (SOUSA, 2006, p. 5). Jardim assevera, de maneira sintética, que se pode entendê-las como um...

[...] conjunto de premissas, decisões e ações - produzidas pelo Estado e inseridas nas agendas governamentais em nome do interesse social - que contemplam os diversos aspectos (administrativo, legal,



científico, cultural, tecnológico, etc.) relativos à produção, uso e preservação da informação arquivística de natureza pública e privada. (JARDIM, 2003, p. 38-39).

Políticas públicas arquivísticas constituem uma das dimensões das políticas públicas informacionais. Por serem parte integrante do contexto informacional, as políticas voltadas para a questão dos arquivos deveriam dialogar com outros processos do campo informacional, compartilhando e recebendo recursos, com vistas à sua consolidação. Normalmente, na realidade brasileira não há articulação das várias ações das políticas de informação. Talvez esteja aí uma das razões para os insucessos, nos níveis macro e institucional, das políticas de arquivo:

Em função da realidade observada, é possível detectar situações nas quais políticas públicas arquivísticas são concebidas e implementadas - normalmente sem muito sucesso - ignorando-se as demais políticas públicas de informação existentes. Da mesma forma, são frequentes situações nas quais políticas públicas de informação - muitas vezes em nível nacional - desconhecem por completo as peculiaridades do universo arquivístico (JARDIM, 2011, p. 200).

Adão (2017) alerta para a ampla utilização, sem a necessária distinção, das expressões política de arquivos e política pública de arquivos. No entendimento da autora, “política de arquivos é aquela que orienta o estabelecimento das linhas de trabalho de determinado serviço arquivístico, público ou privado”, diferindo-a de uma “política pública de arquivos” por não resultar da atividade política e, por conseguinte, da ação do Estado, mas de “decisões internas que são tomadas pelos gestores considerando-se as metas e objetivos do arquivo e, conseqüentemente, da instituição que o abriga” (ADÃO, 2017, p. 120).

Em suma, “política de arquivos” refere-se ao âmbito interno de uma instituição e “políticas públicas de arquivo”, ao amplo espectro em que Estado e sociedade se articulam para alcançarem objetivos comuns em torno dos arquivos. Mesmo no âmbito interno, porém, pode haver políticas institucionais de diferentes matizes, sendo necessário especificá-las e, quando se tratar de arquivos, nomeá-la como “política institucional de arquivos”.

Em uma rápida busca nas plataformas Google Search e Google Acadêmico realizada em 4 de novembro de 2018, obtiveram-se os seguintes resultados, somente na língua portuguesa, para as duas expressões (Tabela 1):

Tabela 1 – Buscas na plataforma Google

Expressão	Google Search (resultados)	Google Acadêmico (resultados)
“política institucional de arquivos”	21	11
“políticas públicas arquivísticas”	2.820	222
“políticas públicas de arquivos”	57.700	245

Fonte: Dados da pesquisa.

A literatura sobre o tema ainda é escassa e carece de aprofundamento. Vários autores (alguns citados neste trabalho) utilizam as duas expressões como se fossem equivalentes. Na ausência de especificação, há que se ater ao contexto em que uma ou outra expressão foi utilizada. Para o norte desta pesquisa, é importante esclarecer que ela se preocupou com a “política pública de arquivos”, com a “política institucional de arquivos” e com a gestão documental, o que, em última análise, independe da definição dessas políticas.

As instituições desempenham papel decisivo em toda política pública, emanando ou condicionando as principais decisões. “Sua estrutura, seus quadros e sua cultura organizacional são elementos que configuram a política” (SARAVIA, 2006, p. 37). Por essa razão, é necessário compreender sua estrutura, seu comportamento interno e, ainda, o contexto em que se situa, para só depois se elaborar uma política, programa ou projeto que visem a inovações, alterações ou melhorias.

Indolfo (2015, p. 11) afirma sobre as políticas arquivísticas (leia-se “políticas públicas arquivísticas”) que elas “não são produtos ou consequências da entrada em vigor de um ato legal ou normativo; elas são frutos de vontades, decisões e recursos que envolvem a presença e atuação do Estado e da sociedade”. Para que se alcancem os objetivos e metas almejados, uma política pública de arquivos deve

se munir de uma série de instrumentos, como programas, projetos, recursos orçamentários e pessoal com conhecimento técnico e habilidades políticas, além, é claro, da legislação arquivística.

Para Jardim, a legislação arquivística tende a ser considerada o marco zero de uma nova era arquivística, mas, isoladamente, não garantirá a implementação de uma política. Jardim (2003, p. 43) também previne que “uma legislação ignorada pela sociedade e o Estado pode ser tão perniciosa quanto a falta dela”, sendo necessário que se torne conhecida pelo universo dos arquivos, pelos diversos setores do Estado e pela sociedade.

No Brasil, há fundamentação legal que versa sobre as várias temáticas que envolvem arquivos, documentos e informação. A questão é tratada em todos os níveis de hierarquia das normas jurídicas, da Carta Magna às resoluções, detalhando diretrizes, sistemas, programas, procedimentos e regras a serem implementados. No entanto, em que pese a existência de legislação, não é possível admitir que haja uma política nacional de arquivos, uma vez que faltam programas e projetos que assegurem sua implementação e desenvolvimento.

De qualquer modo, a legislação existe e é instrumento norteador e legitimador de políticas arquivísticas públicas ou institucionais. Não é objetivo desta pesquisa fazer um levantamento exaustivo de toda a legislação arquivística brasileira e analisá-la em profundidade. Outros autores o fizeram recentemente. A proposta aqui é tanger as normas mais importantes que afetam diretamente o universo das IFES, com ênfase na gestão de documentos.

A Constituição Federal de 1988 (BRASIL. Constituição, 1988), em seu art. 216, §2º, determina que “cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem”. A expressão na forma lei significa que o preceito deveria ser explicitado por lei infraconstitucional. Foi o que ocorreu com a publicação, três anos depois, da Lei Federal n. 8.159, de 8 de janeiro de 1991 (BRASIL. Presidência da República, 1991), que dispõe sobre a política nacional de arquivos públicos e privados. Tal Lei, também chamada “Lei de Arquivos”, foi responsável pela institucionalização da gestão de documentos no Brasil (MORENO, 2008, p. 85). Em seu art. 1º, ela estabelece que a “gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação” (BRASIL. Presidência da República, 1991) é dever do Poder Público.

A Lei de Arquivos gerou a expectativa de profundas mudanças no cenário arquivístico brasileiro. De fato, segundo Jardim (2013b), pela primeira vez no País, uma lei assegurou a concepção de um regime jurídico em que foram configurados atores e processos, com o envolvimento do Estado e da sociedade, relacionados às políticas e formas de gestão das informações arquivísticas governamentais. Apesar das dificuldades de implantação, Jardim avalia que a lei trouxe avanços significativos:

- o início da ruptura com o modelo de arquivo histórico, atrelado a uma perspectiva patrimonialista, que caracterizava a maior parte das instituições arquivísticas brasileiras;
- a definição da autoridade arquivística dos arquivos públicos brasileiros como gestores do ciclo vital de documentos arquivísticos, desde a sua produção à destinação final, nas diversas esferas da administração pública;
- a introdução da gestão de documentos como instrumento de racionalidade e transparência da administração pública sob a ação político-normativa das instituições arquivísticas públicas (JARDIM, 2013b, p. 384).

A Lei de Arquivos instituiu o Sistema Nacional de Arquivos (SINAR) e criou o Conselho Nacional de Arquivos (CONARQ), órgão central do SINAR, vinculado ao Arquivo Nacional. Em seu regulamento, o Decreto n. 4.073, de 3 de janeiro de 2002 (BRASIL. Presidência da República, 2002), estão listados os órgãos que integram o SINAR, bem como sua finalidade, que é “implementar a política nacional de arquivos públicos e privados, visando à gestão, à preservação e ao acesso aos documentos de arquivo.” O decreto estabeleceu, também, as competências do CONARQ e como sua finalidade “definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo”. Dentre outras determinações, ainda prescreve em seu Capítulo VI, art. 18:

Em cada órgão e entidade da Administração Pública Federal será constituída comissão permanente de avaliação de documentos, que terá a responsabilidade de orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor (BRASIL. Presidência da República, 2002).

A eliminação de documentos arquivísticos produzidos por instituições públicas e de caráter público só será permitida se aqueles passíveis de eliminação forem submetidos à avaliação de uma Comissão Permanente de Avaliação de Documentos (CPAD) no âmbito dessas instituições e, posteriormente, após autorização de instituição arquivística pública, em sua esfera de competência. Assim, no caso das IFES, a autorização deve ser concedida pelo Arquivo Nacional.

Referências normativas importantes também são aquelas que tratam dos instrumentos de gestão de documentos. A Resolução n. 14 do CONARQ, de 24 de outubro de 2001 (BRASIL. Ministério da Justiça. CONARQ, 2001), aprovou a versão revisada e ampliada da Resolução n. 4, de 28 de março de 1996, que dispõe sobre o código de classificação de documentos de arquivo e a tabela de temporalidade e destinação de documentos de arquivo relativos às atividades-meio da Administração Pública a serem adotados pelos órgãos e entidades integrantes do SINAR.

Já a Portaria n. 92, de 23 de setembro de 2011 (BRASIL. CONARQ, 2011a), aprovou o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-Fim das Instituições Federais de Ensino Superior (IFES). Em 2013, a obrigatoriedade de utilização desses instrumentos por essas instituições de ensino foi determinada pela Portaria MEC n. 1.261, de 13 de dezembro de 2013 (BRASIL. Ministério da Educação - MEC, 2013).

Outro importante marco legislativo foi a publicação da Lei n. 12.527, de 18 de novembro de 2011 (BRASIL. Presidência da República, 2011), que dispõe sobre os procedimentos a serem observados pela União, estados, Distrito Federal e municípios, com o fim de garantir o acesso a informações previsto na Constituição. A chamada “Lei de Acesso à Informação” (LAI) estabelece, em seu art. 5º, que é “dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão”. Em seu art. 3º (talvez o mais emblemático), estabelece as seguintes diretrizes para os procedimentos previstos em seu texto, que têm como objetivo assegurar o direito fundamental de acesso à informação:

- I - observância da publicidade como preceito geral e do sigilo como exceção;
- II - divulgação de informações de interesse público, independentemente de solicitações;
- III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
- IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
- V - desenvolvimento do controle social da administração pública (BRASIL. Presidência da República, 2011).

A proposta da LAI é norteadada pela transparência, que deve prevalecer sobre a opacidade do Estado. A partir desta Lei, os órgãos e entidades do Poder Público passaram a contar com Serviços de Informação ao Cidadão (SIC), como previsto em seu art. 9º. Qualquer cidadão interessado pode ter acesso à informação que lhe é necessária em prazo determinado e sem a obrigatoriedade de apresentar justificativa. A questão do acesso à informação eleva-se a um patamar inédito, cabendo aos atores e à sociedade contribuírem para o enraizamento da cultura de transparência, fiscalização e controle social da Administração Pública.

De acordo com Indolfo (2015, p. 11-12), a elaboração de leis, regulamentos, normas e diretrizes por agentes do Estado responsáveis pela Política Nacional de Arquivos foi uma tentativa de oferecer instrumental técnico-científico para solucionar o “caos documental” existente nas instituições arquivísticas e nos serviços de arquivo. A normalização empreendida desde a promulgação da Lei de Arquivos visou à harmonização técnica e à uniformização da terminologia e do aspecto jurídico-discursivo da produção de normas arquivísticas no Brasil. No entanto, afirma Indolfo, da capacitação técnica e do domínio de certas habilidades por parte dos servidores/agentes públicos e demais recursos humanos lotados nos serviços arquivísticos depende a efetiva aplicação da legislação. Pode-se acrescentar que, além do essencial domínio técnico, as outras habilidades a que se refere a autora podem significar habilidade

política, para negociar o enfrentamento das dificuldades, conquistando-se espaços, recursos e aliados, e habilidade pedagógica, para difundir o conhecimento arquivístico, com vistas à sensibilização, ao convencimento e à introjeção de uma consciência ou cultura arquivística.

Em 12 de dezembro de 2003, foi publicado o Decreto n. 4.915 (BRASIL. Presidência da República, 2003), que dispõe sobre o Sistema de Gestão de Documentos de Arquivo (SIGA), da Administração Pública Federal. O Arquivo Nacional é um dos integrantes desse sistema e nele exerce a função de Órgão Central. Também o integram órgãos setoriais (ministérios e órgãos equivalentes) e órgão seccionais (unidades vinculadas aos ministérios e equivalentes). O Decreto define a finalidade do SIGA em seu art. 2º:

I - garantir ao cidadão e aos órgãos e entidades da administração pública federal, de forma ágil e segura, o acesso aos documentos de arquivo e às informações neles contidas, resguardados os aspectos de sigilo e as restrições administrativas ou legais;

II - integrar e coordenar as atividades de gestão de documentos de arquivo desenvolvidas pelos órgãos setoriais e seccionais que o integram;

III - disseminar normas relativas à gestão de documentos de arquivo;

IV - racionalizar a produção da documentação arquivística pública;

V - racionalizar e reduzir os custos operacionais e de armazenagem da documentação arquivística pública;

VI - preservar o patrimônio documental arquivístico da administração pública federal;

VII - articular-se com os demais sistemas que atuam direta ou indiretamente na gestão da informação pública federal (BRASIL. Presidência da República, 2002).

A criação do SIGA representou um passo importante e necessário para a organização das atividades de gestão de documentos no âmbito dos órgãos e entidades da Administração Pública Federal. Contudo, Venâncio constata:

Nos dias atuais, de forma semelhante a várias instituições públicas brasileiras, os arquivos das IFES se encontram em graus variados de organização. Há numerosos casos de completo abandono, em que funcionários sem treinamento eliminam aleatoriamente séries documentais e/ou promovem o acúmulo de massas documentais em depósitos inapropriados (VENÂNCIO, 2015, p. 36).

A superação dessas situações está entre as propostas do SIGA. Por meio da promoção de reuniões e encontros nacionais para a discussão da legislação, projetos e pesquisas no campo da Arquivologia, o SIGA tem aproximado os integrantes em uma linguagem única, identificando problemas e buscando soluções. Merece destaque como um dos bons produtos gerados a partir da parceria entre os técnicos do Arquivo Nacional e representantes das IFES a criação, em 2011, do Código de Classificação e a Tabela de Temporalidade relativos às atividades-fim das IFES (SANTOS JÚNIOR, 2017, p. 56-57).

#### Documentos, arquivo e gestão

O boom informacional ocorrido após a Segunda Guerra Mundial teve como consequência o crescimento exponencial da produção de documentos e o surgimento de grandes massas documentais, o que implicou novos problemas, que exigiram soluções inéditas. Juntam-se a esse fator as contínuas alterações das estruturas burocráticas ocorridas a partir do mesmo período e ter-se-á noção da complexidade dos desafios enfrentados pelos arquivistas naquele período concernentes ao contexto de criação e uso dos documentos e à transmissão desse conhecimento ao público consulente (DINGWALL, 2016, p. 205). Nesse contexto, não no domínio da Arquivologia, mas sim no da Administração Científica, é que surge a gestão de documentos:

A aplicação dos princípios da administração científica para a solução dos problemas documentais gerou os princípios da gestão de documentos, os quais resultaram, sobretudo, da necessidade de se racionalizar e modernizar as administrações. Não se tratava de uma demanda setorializada, produzida a partir das próprias instituições arquivísticas, em que pese as consequências extremamente inovadoras que trouxeram para a arquivologia (JARDIM, 1987, p. 36).



Os pioneiros na elaboração do conceito de gestão de documentos (record management) foram os países anglo-saxônicos. A perspectiva era, a princípio, ...

[...] nitidamente mais administrativa e econômica do que arquivística, uma vez que se tratava, essencialmente, de otimizar o funcionamento da administração, limitando a quantidade de documentos produzidos e o prazo de guarda [...] (INDOLFO, 2007, p. 30-31).

De acordo com Moreno (2008, p. 82), a palavra gestão pode ser entendida como “ação ou efeito de administrar, ou seja, é toda a atividade dirigida com o objetivo de obter e administrar os recursos necessários para o cumprimento dos objetivos, de qualquer organização”. Administrar documentos, portanto, significa administrar recursos informacionais essenciais aos objetivos e à própria existência das organizações. Mas, se o termo gestão relaciona-se a administrar, gerenciar, o que significa documento e o que justifica todo o aporte técnico-científico a partir dele construído?

### Documento

Em sentido amplo, documento pode ser entendido como a informação que está registrada em qualquer suporte ou formato. “É qualquer elemento gráfico, iconográfico, plástico ou fônico pelo qual o homem se expressa”, explica Bellotto (2014, p. 35). Assim, pode ser um livro, um artigo de jornal ou revista, uma ata, um relatório, um ofício, um processo, um mapa, uma fotografia, uma pintura, um filme, uma escultura etc. A autora afirma que a determinação da condição de um documento como de arquivo, biblioteca, museu ou centro de memória não ocorre em razão de seu suporte, mas sim de sua origem e de sua utilização. Roncaglio, Szvarça e Bojanoski (2004, p. 1) também destacam os vários sentidos da palavra:

Documento é um termo também polissêmico, posto que se pode considerar documento qualquer suporte que registre informações. São documentos as camadas da terra escavadas pelos geólogos, os vestígios materiais de civilizações desaparecidas investigados pelos arqueólogos, os registros orais de grupos humanos estudados pelos antropólogos e sociólogos ou a correspondência, mapas, contratos privados ou públicos que são pesquisadas pelos historiadores.

Dadas as múltiplas possibilidades de aplicação do termo documento em sentido lato, é pertinente especificar “documento de arquivo” a partir das motivações para sua criação e utilização. São documentos de arquivo ou arquivísticos<sup>17</sup> “aqueles que, produzidos e/ou recebidos por pessoa física ou jurídica, pública ou privada, no exercício de suas atividades, constituem elementos de prova ou de informação” (BRASIL, Arquivo Nacional, 2011). Eles surgem em razão da necessidade de seu produtor expressar determinado ato no exercício de suas atividades e funções. Em outras palavras, são a materialização das manifestações de seu produtor registradas em qualquer suporte e cuja utilidade é probatória e também informativa.

Ao contrário dos outros documentos, os arquivísticos nascem como provas e, por isso mesmo, sob os auspícios da legislação arquivística e correlata, de maneira que sua destruição em desacordo com as normas configura crime. “Documentos de arquivo são provas. Nascem como provas, permanecem como testemunhos” (BELLOTTO, 2014, p. 179). No entender de Camargo (2009, p. 426)

[...] os documentos de arquivo, como subprodutos de atividades praticadas por instituições e indivíduos no cumprimento de suas funções, de acordo com os padrões jurídicos da sociedade em que se inserem, já nascem com estatuto probatório. São os ‘documentos de nascença’, como os rotulou Marie-Anne Chabin (1999), e não se confundem com os de ‘batismo’, isto é, os que recebem estatuto probatório única e exclusivamente por força das operações a que são submetidos por juristas, historiadores e outros interessados, no propósito de fundamentar sentenças, teses e decisões.

O documento arquivístico também se distingue por aspectos que lhe são peculiares e, ainda, por sua relação com a entidade que o produziu. Rodrigues (2003, p. 219) sintetiza o pensamento de Duranti (1994)<sup>18</sup> ao enumerar e descrever cinco características básicas que os documentos de arquivo devem possuir para serem considerados como tal:

- Imparcialidade - são produzidos dentro de determinado contexto e para determinados fins;
- Autenticidade - são criados, mantidos e conservados sob custódia de acordo com procedimentos regulares que podem ser comprovados;

- Naturalidade - são produzidos e acumulados no curso de transações e de acordo com as necessidades do assunto tratado;
- Inter-relacionamento - estabelecem relações entre si e com as atividades que os geraram;
- Unicidade - cada registro arquivístico tem um lugar único na estrutura documental do conjunto ao qual pertence.

A essas características, Santos (2015, p. 116) soma a fixidez, que diz respeito à qualidade de ser estável e, ao mesmo tempo, de ser resistente a mudanças. O autor justifica essa inclusão por entender que a estabilidade está implícita no conceito de documento arquivístico, posto que este não é simples dado ou informação mas é, de outro modo, predominantemente identificado como documento (RON-DINELLI, 2011:19 apud SANTOS, 2015, p. 117).

Com a fixidez assegura-se que o documento tenha sempre a mesma aparência ou apresentação (forma fixa) e que a informação e os dados nele contidos se mantenham imutáveis (conteúdo estável). A fixidez independe do suporte, se analógico ou digital. Contudo, no mundo digital o conteúdo permanece inalterado, ao passo que a forma, no âmbito de uma variabilidade limitada, pode sofrer alterações.

Considerando a fixidez, Santos (2015, p. 116) propõe a seguinte definição para documento arquivístico:

Conjunto de dados estruturados, apresentados em uma forma fixa, representando um conteúdo estável, produzido ou recebido por pessoa física ou jurídica (pública ou privada), no exercício de uma atividade, observando os requisitos normativos da atividade à qual está relacionado, e preservado como evidência da realização dessa atividade.

Quando se trata especificamente de suporte digital, o CONARQ (BRASIL. Arquivo Nacional, 2005), conceitua documento digital como aquele “codificado em dígitos binários, acessível por meio de sistema computacional”. Já o documento arquivístico digital foi assim definido pela Câmara Técnica de Documentos Eletrônicos (CTDE), do CONARQ:

Documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional. São exemplos de documentos arquivísticos digitais: textos, imagens fixas, imagens em movimento, gravações sonoras, mensagens de correio eletrônico, páginas web, bases de dados, dentre outras possibilidades de um vasto repertório de diversidade crescente (BRASIL. CONARQ. CTDE, 2004).

A definição acima foi extraída da primeira versão do glossário elaborado pela CTDE em 2004. Na sétima versão do glossário, publicada em 2016, documento arquivístico digital passou a ser conceituado como “documento digital reconhecido e tratado como um documento arquivístico” (BRASIL. CONARQ. CTDE, 2016). Dessa forma, para se compreender o conceito, deve-se saber o que é documento arquivístico e o que é documento digital. Tais conceitos também foram atualizados em relação à versão de 2004: documento arquivístico passou a ser entendido como o “documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência” e documento digital como a “informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional” (BRASIL. CONARQ. CTDE, 2016).

Com a massificação das Tecnologias da Informação e Comunicação (TICs), os documentos digitais são hoje uma realidade na maioria das instituições e bastante presentes na vida dos indivíduos. Com o “novo” suporte, vieram novos problemas, preocupações e desafios, e a maneira de entender a preservação tomou outro contorno. Acrescente-se à problemática um certo grau de urgência, em virtude da necessidade de se tomar decisões que impeçam a formação de massas documentais digitais e/ou o descarte sem critérios de avaliação. Se não houver controle, a facilidade de se criar documentos digitais é muito grande, tanto quanto a facilidade de se descartar.

Independentemente do suporte, os documentos arquivísticos são criados para cumprir uma função instrumental no âmbito organizacional. É por meio deles que se registram os atos de seu produtor. Possuem valor primário, podendo possuir também valor secundário. É desejável que os cuidados com sua preservação, com vistas à durabilidade do suporte e da informação, tenham início no momento de sua criação. Cruz adverte:

O tratamento dos documentos iniciado nos órgãos administrativos não visa tão somente ao benefício dos usuários das instituições arquivísticas, mas sim, e principalmente, ao benefício da própria organização que os gerou. Em qualquer instituição há um grupo de pessoas que toma decisões e se esforça para que a missão daquele órgão seja cumprida satisfatoriamente. Há, também, um serviço burocrático responsável por executar as decisões tomadas pelos dirigentes. De modo geral, esse corpo burocrático fornece o suporte informacional necessário à tomada de decisão. São os documentos e os arquivos os responsáveis por colocar à disposição as informações necessárias (CRUZ, 2013, p. 12).

O documento arquivístico, portanto, não importa se analógico ou digital, é crucial para o funcionamento e a existência das instituições. É como um fluido que nutre um organismo, dando-lhe força vital, dinamismo e longevidade. Deve, portanto, receber tratamento distinto dos demais documentos, de modo a garantir a manutenção de seus atributos e sua condição de “arquivístico”. Somente assim ele atenderá plenamente aos propósitos para os quais foi produzido e, ainda, poderá servir para usos secundários, alheios à finalidade de sua gênese.

### **Arquivo**

Arquivo é um termo polissêmico, podendo designar a instituição ou o serviço responsável pela guarda, processamento e acesso aos documentos, a edificação que abriga conjuntos documentais ou o móvel destinado à guarda de documentos. À luz da Lei 8.159, de 1991 (BRASIL. Presidência da República, 1991), arquivos são:

[...] conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

Considerando-se essa definição, em se tratando de instituições públicas, um arquivo é resultado da acumulação natural de documentos que foram produzidos ou recebidos por agentes do Poder Público no exercício de suas funções. Destaca-se a acumulação natural desses conjuntos documentais em oposição à intencionalidade que ocorre em outras unidades de informação, como, bibliotecas, centros de memória e museus, que reúnem documentos de maneira artificial para atender aos propósitos de suas atividades.

Um arquivo (conjunto de documentos) tem por finalidade servir à administração, atendendo a suas demandas administrativas, legais, fiscais, e, em um segundo momento, ser útil como fonte de pesquisa e informação para terceiros ou para a própria administração. Bellotto define:

Arquivos são instrumentos, arquivos são ferramentas. Ferramentas da administração (dos órgãos públicos ou das organizações privadas); ferramentas da cidadania (dos direitos e dos deveres dos cidadãos); ferramentas do direito (fontes do exercício jurídico); ferramentas da historiografia (os documentos são os instrumentos de trabalho do historiador); tudo isso, ademais de serem instrumentos indispensáveis da ciência, da tecnologia, do dia a dia das pessoas. Arquivos são instrumentos nos quais a informação está registrada, para que dela se faça uso. ‘O arquivo é ferramenta da administração e é celeiro da história’, já disse o arquivista francês Charles Bautier (BELLOTTO, 2014, p. 179, grifo nosso).

Para que cumpra seu papel de ferramenta útil para diversas necessidades, os documentos que o compõem devem passar por procedimentos e operações técnicas que assegurem sua organização, preservação e utilização.

Arquivo também pode ser entendido como “instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso a documentos” (BRASIL. Arquivo Nacional, 2005, p. 27). Um serviço de arquivo institucionalizado é essencial para o bom funcionamento de qualquer organização. Apesar disso, Bottino alerta:

A criação e organização do arquivo universitário são tarefas árduas, que requerem a adoção de medidas que visem à otimização dos serviços. Para que isso ocorra, a universidade precisa ter consciência da importância da preservação e manutenção de seus arquivos, advinda da percepção do quanto os arquivos organizados podem contribuir para a consecução dos objetivos institucionais, fornecendo informações ágeis, seguras e com qualidade, assegurando a eficiência e a eficácia da organização de ensino, levando-a a cumprir seu papel na sociedade (BOTTINO, 2015, p. 27).

Grande parte das instituições de ensino superior não conta com políticas ou programas de gestão de documentos e arquivos. Torna-se mesmo inadequada a utilização de conceitos que só fazem sentido onde existe administração racional dos documentos. Onde não há gestão de documentos não há que se falar em arquivos correntes, intermediários ou permanentes, por exemplo. Segundo Sousa (1997, p. 2), o que se observa na Administração Pública brasileira é “a formação de dois grandes acervos: os arquivos montados nos setores de trabalho e massas documentais acumuladas”. A alteração desse cenário só será possível mediante a implementação de uma gestão arquivística que deve receber apoio político da administração, bem como recursos financeiros, humanos, materiais e técnicos.

### Gestão de documentos

Rondinelli (2005, p. 40-41) considera cinco marcos históricos para a Arquivologia: a) criação do Arquivo Nacional da França, em 1789; b) criação, em 1821, da École Nationale des Chartes, também na França, o que fortaleceu a Arquivologia como ciência auxiliar da história e a visão culturalista dos arquivos<sup>20</sup>; c) promulgação, em 1841, uma vez mais na França, do princípio da proveniência (ou do respeito aos fundos), inspirada pelo historiador e arquivista francês Natalis du Wailly; d) explosão documental no período pós-Segunda Guerra Mundial, que impacta as instituições com grandes volumes de documentos, dando ensejo à formação de comissões governamentais<sup>21</sup> no Canadá e nos Estados Unidos, culminando com o surgimento do conceito de gestão de documentos; e e) ampla utilização dos documentos eletrônicos a partir da década de 1980, que deu início à revisão de princípios e métodos da Arquivologia.

De fato, a explosão documental é marco importante, pois ocorreu em função dos avanços científicos e tecnológicos alcançados no período pós-Segunda Guerra e deu azo ao surgimento da gestão de documentos. A produção documental superou a capacidade de controle e organização das instituições, que buscaram novas soluções para gerir as massas documentais acumuladas (PAES, 2004, p. 53).

A gestão de documentos impactou fortemente a maneira de se entender e de lidar com documentos. Os próprios arquivos retomariam sua função de apoio à Administração:

O conceito de gestão de documentos restaura e dinamiza a concepção dos arquivos como instrumentos facilitadores da administração, que vigorou até o século XIX, quando, como já vimos, por influência de uma visão dos arquivos apenas como guardiães do passado eles passaram a desempenhar funções de apoio à pesquisa histórica (RONDINELLI, 2005, p. 41).

A história mostra-nos que, a partir do conceito de gestão de documentos ou gestão documental, modifica-se a tradição dos arquivos voltados exclusivamente para servir à pesquisa histórica, iniciando-se o processo de aproximação com a administração, na medida em que a gestão estabelece medidas e rotinas, visando à racionalização e à eficiência da criação, manutenção, uso e avaliação de documentos arquivísticos (MORENO, 2008, p. 85).

Antes de apresentar as definições de gestão documental, é oportuno trazer à baila os conceitos da Teoria das Três Idades e do modelo do Ciclo Vital dos documentos. O Dicionário Brasileiro de Terminologia Arquivística (BRASIL. Arquivo Nacional, 2005) informa que, com base na Teoria das Três Idades, os arquivos são designados como “correntes”, “intermediários” ou “permanentes”, conforme a frequência de uso pelas entidades que os produziram, e, também, conforme a identificação de seus valores, primário ou secundário.

Já o modelo do ciclo vital foi uma tentativa de explicar a adaptação dos processos de tratamento documental à nova realidade, em que o volume dos documentos passou a ser um grande problema e uma ameaça à eficiência administrativa. Santos (2005, p. 177) define assim o ciclo vital:

A duração da vida de um documento desde sua criação ou recebimento até sua destinação final, caracterizada pela frequência da sua utilização e pelo tipo de uso que deles é feita. O ciclo vital é constituído de três etapas ou fases, que são: ativa ou corrente, semiativa ou intermediária e inativa, permanente ou histórica.

Dingwall (2016) faz uso de duas metáforas para explicar o modelo do ciclo vital. A primeira é a metáfora orgânica, que descreve os estágios da existência temporal de um documento definida pelo “nascimento” (criação) e pela “morte” (extinção) e que sofrem mudanças (crescimento, amadurecimento e decadência) ao longo das fases que percorre.



A outra metáfora é a religiosa, em que o arquivo intermediário é um purgatório, onde os escolhidos esperam pela pós-vida arquivística e os condenados aguardam o abismo do triturador de papel.

A criação do arquivo intermediário foi a solução encontrada para o acúmulo de documentos nos setores de trabalho (DINGWALL, 2016, p. 207).

Os documentos cuja utilização era menos frequente, mas que ainda possuíam valor primário (administrativo, legal e fiscal) passaram a ocupar depósitos mais ou menos próximos aos seus produtores, aguardando a eliminação ou o recolhimento aos depósitos de arquivo permanente.

Em resumo, o ciclo vital diz respeito às diferentes fases que o documento percorre, da criação à destinação final, passando pela fase intermediária. Explicita Dingwall:

O modelo do ciclo vital é uma representação linear dos estágios da existência de um documento, começando com sua criação em algum departamento de alguma entidade e terminando com a destruição ou com sua preservação permanente em algum arquivo (DINGWALL, 2016, p. 209).

O advento das TICs provocou o surgimento de novos modos de produção, uso e conservação dos documentos arquivísticos, o que, relacionado às mudanças na gestão das organizações, confrontou as teorias e métodos da Arquivologia e, mesmo, a formação e o perfil do arquivista. Esse cenário dá ensejo à emergência, na Austrália, em meados da década de 1990, da teoria, ou modelo, do records continuum (JARDIM, 2015, p. 35).

O modelo do ciclo vital teria se tornado insuficiente para explicar a nova realidade. Segundo Dingwall (2016, p. 206), as inadequações do ciclo vital se referiam a como esse modelo descrevia o trabalho técnico e também a sua incapacidade de lidar com o incipiente problema produzido pelos documentos digitais.

Critica-se, entre outras coisas, a pouca flexibilidade do modelo do ciclo vital, pois a divisão estancada em fases ou idades restringe a aplicabilidade das funções, procedimentos e operações arquivísticas, o que, no documento digital pode ser executado a qualquer momento ou fase do documento, sem necessariamente ter que obedecer ao impositivo do tempo.

A descrição, por exemplo, poderia se dar a qualquer momento, e não obrigatoriamente na fase permanente. Costa Filho compreende...

[...] a visão fornecida pelo records continuum como fundamental para a elucidação das limitações impostas pelo ciclo vital dos documentos. As possibilidades fornecidas pelos documentos arquivísticos digitais são incomensuráveis e quaisquer fatores restritivos, no nosso entendimento, não permitirão que seu usufruto seja integral. O caráter espaço-temporal do continuum rompe com a linearidade e o engessamento impostos pelas fases do ciclo vital (COSTA FILHO, 2016, p. 166).

Santos (2015, p. 171) argumenta que, ao contrário do que pensam os defensores do records continuum, essa abordagem de acompanhamento contínuo dos documentos arquivísticos é uma nova interpretação do ciclo vital e o reafirma como princípio arquivístico, não se consubstanciando, portanto, em um novo paradigma capaz de substituí-lo. O autor ainda afirma que:

a prática brasileira, por exemplo, serve para demonstrar que o conceito [do ciclo vital] evoluiu ao longo das décadas, afinal, apesar de não reconhecer o records continuum como paradigma brasileiro de tratamento de documentos arquivísticos, muitas das características reputadas a ele estão incorporadas ao entendimento do ciclo vital adotado no país (SANTOS, 2015, p. 173).

As discussões sobre o records continuum na literatura arquivística ainda é recente e escassa. O próprio Dicionário Brasileiro de Terminologia Arquivística (BRASIL. Arquivo Nacional, 2005) e a última versão do glossário da CTDE (BRASIL. CONARQ. CTDE, 2014) não fazem menção ao termo, mas se trata de um campo profícuo para debates, que devem se acentuar à medida que no Brasil o documento digital supere em utilização o analógico.

De acordo com Indolfo (2007, p. 35), a UNESCO, em 197922, estabeleceu o Records and Archives Management Program (RAMP), programa concebido para tentar alertar o público geral e os tomadores de decisão para a importância dos documentos e arquivos e, ainda, assessorar os governos a estabelecerem infraestruturas eficientes para a gestão de documentos.

Ainda segundo Indolfo (2007), a diversidade de modelos existente no âmbito internacional levou a UNESCO, por meio do RAMP, a propor a seguinte definição para o conceito de gestão de documentos: “domínio da gestão administrativa geral com vistas a assegurar a economia e a eficácia das operações desde a criação, manutenção e utilização, até a destinação final dos documentos” (INDOLFO, 2007, p. 36).

A Lei n. 8159 de 1991 define, em seu art. 3º, a gestão de documentos como o “conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente” (BRASIL. Presidência da República, 1991). Nesta definição encontra-se a essência do ciclo vital: as fases documentais. Llansó Sanjuan afirma:

A chave para a definição do conceito de gerenciamento de documentos está na noção do ciclo de vida dos documentos, denominada em sua origem de teoria das três idades, que corresponde a documentos ativos, semi-ativos e inativos.

O objetivo de sua formulação é garantir a presença do arquivista e dos métodos que aplica para que a documentação receba o tratamento adequado em cada uma das idades (LIANSÓ SANJUAN, 2006, p. 42, tradução nossa).

Camargo e Bellotto (1996) não incluem o ciclo vital em sua proposta de conceituação, mas acrescentam a racionalização e a eficiência como objetivos. As autoras se referem assim à gestão documental:

Conjunto de medidas e rotinas que tem por objetivo a racionalização e eficiência na produção, tramitação, classificação, avaliação, arquivamento, acesso e uso das informações registradas em documentos de arquivo.

Fatores como a especificidade das tradições arquivísticas ou administrativas e, ainda, o contexto histórico e institucional foram determinantes para a elaboração e desenvolvimento do conceito de gestão de documentos. Portanto, não se pode falar em uma definição única ou universal (INDOLFO, 2007, p. 33-34).

Em 2015, Jardim publicou um estudo que, entre outras coisas, traz um levantamento das definições (22 ao todo) do termo gestão de documentos em diferentes idiomas e tradições arquivísticas. As definições foram extraídas exclusivamente de glossários e dicionários de arquivologia e o autor destaca alguns termos associados a objetos, ações e objetivos da gestão de documentos, indicando semelhanças e diferenças (Quadro 1):

Quadro 1 – Termos extraídos de conceitos de gestão de documentos

Língua	Países/Região	Objeto	Ações	Objetivos
Inglêsa	EUA, Inglaterra, Canadá, Austrália	Produção, manutenção, uso e destinação	Planejamento, controle e direção	Economia e eficiência
Francesa	França, Quebec	Produção, conservação, uso e destinação	Controle	Eficácia (mencionado apenas uma vez)
Espanhola	Colômbia, Costa Rica, Espanha, México	Produção, uso, manutenção, conservação, controle físico e intelectual de documentos íntegros, autênticos e confiáveis	Controle, planejamento, análise da produção, tramitação, uso e informação contida nos documentos	Eficiência, estabelecimento de normas
Portuguesa	Brasil, Portugal	Produção, tramitação, classificação, uso, avaliação e arquivamento	Controle	Eficácia, eficiência e racionalização

Fonte: Elaborado pelo autor a partir de JARDIM (2015).

As diferenças advêm das características intrínsecas a cada tradição arquivística e/ou administrativa e, ainda, da própria terminologia, que costuma variar de acordo com o idioma. Em que pese a algumas

diferenças, a partir dos termos extraídos percebe-se certa convergência na direção de uma administração racional dos documentos com vistas à economia, à eficiência e à eficácia, passando pelo planejamento e controle da produção e pela utilização dos documentos.

Quanto aos objetivos da gestão de documentos, Bernardes e Dellatorre (2008, p. 8-9) assim os sintetizam:

- Assegurar o pleno exercício da cidadania;
- Agilizar o acesso aos arquivos e às informações;
- Promover a transparência das ações administrativas;
- Garantir economia, eficiência e eficácia na administração pública ou privada;
- Agilizar o processo decisório;
- Incentivar o trabalho multidisciplinar e em equipe;
- Controlar o fluxo de documentos e a organização dos arquivos;
- Racionalizar a produção dos documentos;
- Normalizar os procedimentos para avaliação, transferência, recolhimento, guarda e eliminação de documentos;
- Preservar o patrimônio documental considerado de guarda permanente.

As instituições devem investir na consecução desses objetivos e na transformação da realidade atual, a partir de uma mudança cultural na maneira de se perceber e tratar os documentos. Os ganhos proporcionados pela gestão de documentos são grandes e justificam os esforços a serem empreendidos para se atingir os fins colimados.

### **Fases da gestão documental**

Um dos produtos do RAMP foi o trabalho de James Berton Rhoads, publicado em 1983, “A função da gestão de documentos e arquivos nos sistemas nacionais de informação”. Nele, o autor caracteriza um programa de gestão de documentos, especificando as fases e os elementos que devem compô-lo, e propõe níveis de implantação. Sua proposta, afirma Indolfo (2007, p. 36), está entre as mais bem aceitas nos cenários nacional e internacional.

Para Rhoads (1983), a primeira fase da gestão de documentos consiste na produção, que se adequadamente realizada, evitará a criação desnecessária de documentos, diminuindo, assim, o volume documental, o que potenciará o uso e a utilidade dos documentos que realmente são necessários e garantirá que se recorra à reprografia e à automação em um nível racional.

A segunda fase é a utilização que inclui o uso, o controle e o armazenamento de documentos necessários para as funções ou atividades da organização. É caracterizada por medidas voltadas para se assegurar a disponibilidade de informações e documentos úteis, pelo baixo custo de utilização de informações e documentos e pela seleção de material auxiliar, equipamentos e local de armazenamento apropriados à frequência e natureza de seu uso.

A última fase é a destinação, processo crítico em que se deve decidir que documentos serão mantidos como testemunho e quais devem ser destruídos. Neste caso, por quanto tempo eles devem ser guardados em função de seu valor administrativo ou legal. Sugere o autor estadunidense que esse processo deve contar com a participação do arquivista e do gestor de documentos.

### **Níveis/requisitos da gestão documental**

Em seu importante trabalho, James Rhoads definiu quatro níveis de aplicação para um programa de gestão de documentos governamental, salientando que qualquer um dos três primeiros níveis pode ser

acrescido pelos serviços e sistemas dos níveis mais altos. O Quadro 2 apresenta os quatro níveis da gestão de documentos, revelando as exigências mínimas de cada um.

Quadro 2 – Níveis da gestão de documentos

Nível	Sistemas e serviços
Mínimo	<ul style="list-style-type: none"> <li>• sistemas para elaborar programas de retenção e eliminação de documentos;</li> <li>• procedimentos para eliminação adequada dos documentos;</li> <li>• recolhimento aos arquivos nacionais de documentos considerados de valor permanente.</li> </ul>
Mínimo ampliado	Amplia o nível mínimo com: <ul style="list-style-type: none"> <li>• um ou mais centros de arquivamento intermediário.</li> </ul>
Intermediário	Inclui os dois níveis anteriores e os complementa com: <ul style="list-style-type: none"> <li>• subprogramas básicos que consistem em elaboração e gestão de formulários;</li> <li>• gestão de correspondência e informes;</li> <li>• elaboração de sistemas de arquivo e de recuperação;</li> <li>• gestão de arquivos e programas sobre documentos essenciais.</li> </ul>
Máximo	Compreende todos os outros níveis e acrescenta: <ul style="list-style-type: none"> <li>• gestão de diretrizes, correspondências, telecomunicações e máquinas copiadoras;</li> <li>• sistemas de informação sobre gestão;</li> <li>• análises de sistemas e utilização do processamento de palavras e de textos na geração de correspondências, informes e diretrizes, bem como para preenchimento de formulários;</li> <li>• uso do computador e da reprografia em diversas aplicações.</li> </ul>

Fonte: Baseado em RHOADS (1983, p. 31, tradução nossa).

Desde 2006, o SIGA realiza seminários voltados para gestores e servidores que atuam com gestão de documentos em órgãos ou entidades do Poder Executivo Federal. Tais eventos visam à integração, comunicação e divulgação do sistema.

Em sua última edição (VI Seminário do SIGA), realizada em junho de 2018, foi apresentada uma escala de avaliação.

A exemplo da proposta de James Rhoads (1983), foram definidos níveis de maturidade da gestão de documentos a serem aplicados no diagnóstico dos órgãos e entidades que integram o sistema.

Entretanto, o instrumento elaborado pelo SIGA se mostra mais atual e, por essa razão, com maior capacidade explicativa. A gradação ascende do nível mais elementar (1) ao mais completo (5) (Quadro 3):

Quadro 3 – Escala dos níveis de maturidade da gestão de documentos

Nível	Descrição
1	<p>O órgão ou entidade:</p> <ul style="list-style-type: none"> <li>• possui CPAD;</li> <li>• possui protocolo central e/ou protocolo(s) setorial(ais);</li> <li>• possui unidades protocolizadoras;</li> <li>• controla o recebimento, a tramitação e a expedição.</li> </ul>
2	<p>O órgão ou entidade:</p> <ul style="list-style-type: none"> <li>• possui política de gestão de documentos definida que contemple a produção, o arquivamento, a preservação e a segurança dos documentos arquivísticos;</li> <li>• classifica, organiza e avalia seus documentos relativos às atividades-meio com base na Resolução n. 14 do CONARQ;</li> <li>• possui normas internas orientando os procedimentos para eliminação de documentos;</li> <li>• elimina documentos relativos às atividades-meio de acordo com os procedimentos e recomendações do CONARQ.</li> </ul>
3	<p>O órgão ou entidade:</p> <ul style="list-style-type: none"> <li>• possui normas internas para: produção, número de vias/cópias e estabelecimento de modelos de formulários, correspondência e demais documentos avulsos e de procedimentos e rotinas para transferência e recolhimento;</li> <li>• possui processos de trabalho mapeados;</li> <li>• possui arquivo intermediário;</li> <li>• possui TTD-fim aprovada pelo AN;</li> </ul>



	<ul style="list-style-type: none"> <li>• classifica, organiza e avalia documentos relativos às atividades finalísticas;</li> <li>• elimina documentos relativos às atividades finalísticas, de acordo com os procedimentos recomendados pelo CONARQ e AN.</li> </ul>
4	<p>O órgão ou entidade:</p> <ul style="list-style-type: none"> <li>• possui sistema informatizado que apoie o desenvolvimento das atividades de protocolo;</li> <li>• possui sistema informatizado que apoie o desenvolvimento das atividades de gestão de documentos (SIGAD);</li> <li>• possui política de preservação digital definida;</li> <li>• identifica os documentos de arquivo produzidos nos sistemas de negócio que registram as atividades do órgão ou entidade;</li> <li>• trata os documentos de arquivo produzidos nos sistemas de negócio no contexto do programa de gestão de documentos.</li> </ul>
5	<p>No/O órgão ou entidade:</p> <ul style="list-style-type: none"> <li>• o sistema de arquivos está integrado com os sistemas de negócio, o sistema de protocolo e o SIGAD;</li> <li>• não possui documentos, avulsos ou processos, em qualquer suporte, acumulados e sem tratamento técnico;</li> <li>• possui rotinas para a capacitação sistemática dos servidores que atuam nas atividades relacionadas à gestão de documentos, desde a produção até a destinação final;</li> <li>• avalia constantemente e identifica a necessidade de melhorias e alterações no programa de gestão de documentos.</li> </ul>

Fonte: Baseado SIGA... (2018)<sup>28</sup>.

Esta escala foi utilizada na coleta de dados referentes ao exercício de 2017 que serviram para a elaboração do primeiro Diagnóstico Anual do SIGA, apresentado no mesmo seminário. O diagnóstico permitiu conhecer a realidade do Sistema e será útil para sua melhoria, desde que (e este é o propósito) subsidie as políticas, diretrizes, planejamento e programas voltados para a gestão de documentos dos órgãos da Administração Pública Federal.

A escala abrange aspectos relacionados à produção, utilização e destinação dos documentos, ao acervo arquivístico, ao apoio institucional e à adesão à legislação. Trata-se de uma ferramenta que pode ser aplicada individualmente, no âmbito de cada órgão, e é, concomitantemente, um instrumento para descrever a situação arquivística atual, bem como uma referência como projeção para o desenvolvimento institucional relacionado à questão da informação, documentos e arquivos.

Importante destacar que um sistema, órgão ou entidade são compostos, inclusive, por pessoas. A única referência expressa a pessoas na escala está no nível máximo (5), quando menciona a necessidade de capacitação sistemática de servidores. Em momento algum, no entanto, o profissional arquivista é citado. O empreendimento arquivístico, observa Jardim (2003, p. 37, grifo nosso),

[...] requer a construção de uma ordem informacional que pressupõe profissionais especializados, infraestrutura material, conhecimento técnico-científico e gerenciamento adequado de todos esses recursos.

De acordo com Moreno (2008, p. 84), no Brasil a questão dos documentos foi abordada a partir de uma visão mais integrada, “não se acentuando a prática norte-americana em separar o ‘record management’ (gestão de documentos) de ‘archives’ (arquivos permanentes)”. Dessa forma, essa abordagem integrada da Arquivologia no Brasil tem reflexo na formação do profissional, que recebe instruções técnico-científicas para atuar em todo o ciclo vital dos documentos.

O que se pretende aqui destacar é que o arquivista deve ser explicitamente referenciado nas políticas, programas e projetos sobre gestão documental. O tema é polêmico, mas precisa ser discutido (embora não seja este um dos objetivos deste trabalho), pois, se houver disponibilidade de profissional especializado no mercado, não é razoável deixar a questão a cargo de profissionais de outras áreas ou relegada ao “inferno das boas intenções”.<sup>25</sup> Com a inserção e maior exposição do arquivista nas atividades de gestão, ganham o próprio profissional, as instituições formadoras e as contratantes.

### Classificação e avaliação

Os canadenses Rousseau e Couture (1998, p. 265) elencaram sete funções ou operações arquivísticas desenvolvidas ao longo da trajetória documental, que são distintas entre si, mas, de certa forma, possuem relações de continuidade ou se complementam. São elas: criação, avaliação, aquisição, classificação, descrição, conservação e difusão. Todas são importantes para a articulação de um programa de gestão documental. Todavia, para os propósitos desta pesquisa, enfatizar-se-ão a classificação e a avaliação, pois “não há dúvida de que as práticas arquivísticas da classificação e avaliação fundamentam as atividades de gestão de documentos” (INDOLFO, 2007, p. 48).

De acordo com o Dicionário Brasileiro de Terminologia Arquivística (2005), classificação é a “análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos”. Explica Gonçalves:

O objetivo da classificação é, basicamente, dar visibilidade às funções e às atividades do organismo produtor do arquivo, deixando claras as ligações entre os documentos. Podemos entender que a classificação é, antes de tudo, lógica: a partir da análise do organismo produtor de documentos de arquivo, são criadas categorias, classes genéricas, que dizem respeito às funções/atividades detectadas (estão elas configuradas ou não em estruturas específicas, como departamentos, divisões, etc.) (GONÇALVES, 1998, p. 12, grifo da autora).

Segundo Sousa (2013, p. 85), trata-se de um processo que pode ser dividido em uma parte intelectual e outra física. A intelectual compõe-se da classificação propriamente dita (processo mental de estabelecimento de classes), da ordenação (distribuição dos documentos nas classes) e da codificação. A parte física é o arquivamento dos documentos em um local orientado pela classificação e por uma ordem definida.

Lopes também entende que a classificação possui uma dimensão intelectual e outra física, referentes à ordenação dos documentos com base em uma hierarquização das informações neles contidas:

Esta hierarquia se consubstancia em planos e quadros de classificação e em normas gerais de procedimentos derivadas do conhecimento da fonte produtora, das informações acumuladas e dos aspectos materiais e intelectuais do acervo. Portanto, a classificação consiste em uma tentativa de representação ideológica das informações contidas nos documentos (LOPES, 2014, p. 269).

Classificar documentos de arquivo diz respeito à organização em classes do conjunto documental, levando-se em conta as funções, as atividades, o conteúdo e o contexto de produção, o que requer profundo conhecimento do universo a ser classificado. Tal conhecimento possibilita a verificação de vínculos entre os conteúdos e a elaboração de uma estrutura de taxonomia para representações das funções de determinada entidade. É desejável que a base seja as funções, porque estas são alteradas eventualmente e de maneira pontual, ao contrário da estrutura organizacional, que sofre mudanças com relativa frequência.

Santos (2013) afirma que a taxonomia representa uma classificação sistematizada e hierarquizada e recorre a Terra para explicar:

O processo de classificação e organização de informações corporativas é fundamental tanto para a preservação da memória organizacional como para facilitar a contribuição individual. Este processo exige, no entanto, pessoas com habilidades na construção e manutenção de taxonomias organizacionais e que trabalhem em grande sintonia com os principais usuários e produtores de informação e conhecimento (TERRA, 200726 apud SANTOS, 2013, p. 209).

No entender de Santos (2013, p. 180), classificação...

[...] refere-se à criação e à utilização de planos de classificação que reflitam as funções, atividades e ações ou tarefas da instituição acumuladora dos documentos arquivísticos nas fases corrente e intermediária e a elaboração de quadros de arranjo da fase permanente; a classificação orienta a organização intelectual do acervo de forma a refletir a estrutura organizacional e decisória da instituição acumuladora e facilita o acesso aos documentos produzidos; [...].

Para Bernardes e Delatorre (2008, p. 14), os objetivos e os benefícios da classificação são:

- Organização lógica e correto arquivamento de documentos;
- Recuperação da informação ou do documento;
- Recuperação do contexto original de produção dos documentos;
- Visibilidade às funções, subfunções e atividades do organismo produtor;
- Padronização da denominação das funções, atividades e tipos/séries documentais;

- Controle do trâmite;
- Atribuição de códigos numéricos;
- Subsídios para o trabalho de avaliação e aplicação da Tabela de Temporalidade.

Resultado da atividade de classificação, em que é realizado um levantamento do contexto de produção dos documentos de arquivo, o Plano de Classificação agrupa os documentos de acordo com o órgão produtor, a função, a subfunção e a atividade responsável por sua produção ou acumulação, com o objetivo de organizar os arquivos e possibilitar o surgimento de condições para recuperar a informação de forma rápida, segura e eficaz. Trata-se, então, de um...

[...] esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborados a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido. Expressão geralmente adotada em arquivos correntes (BRASIL. Presidência da República, 2005).

Sua elaboração é tarefa extremamente importante, de difícil e morosa execução, decisiva para o bom funcionamento do arquivo. Tal tarefa deve ser realizada de forma acurada, para não dar margem a erros que refletirão na estrutura do arquivo. Há que se levar em conta, ainda, o dinamismo da documentação e prever possibilidades de novas inclusões. Por esta razão, esse instrumento deve ser monitorado constantemente e revisto de tempos em tempos, para atualização e correção de possíveis erros. Sua manutenção e atualização devem ser baseadas em alguns indicadores:

- 1) A quantidade de usuários que não encontram os documentos que procuram;
- 2) Os documentos e categorias que têm volume de acessos muito acima ou abaixo da média;
- 3) Número de documentos não categorizados automaticamente;
- 4) Número de documentos presentes nas diversas categorias, bem como seu crescimento e diminuição no tempo. Os resultados obtidos podem indicar necessidade de reestruturação da árvore, alteração de regras para alocação de documentos, etc. (TERRA et al., 2006:27 apud SANTOS, 2013, p. 210).

Um Plano de Classificação deve satisfazer às necessidades práticas do serviço, utilizando-se de critérios que efetivamente possibilitem a resolução dos problemas. Suas regras de classificação devem ser simples, para melhor se proceder à ordenação dos documentos, e sua construção deve basear-se nas atividades do órgão/entidade e, em último caso, focar a estrutura das entidades.

Segundo Santos (2013, p. 211), “o uso de estruturas taxonômicas [...] tem profunda relação com os planos de classificação”. Desde que bem elaborado, será um instrumento importantíssimo para a gestão dos documentos de arquivo, devendo ser utilizado no início do ciclo vital, pois impactará positivamente as outras funções arquivísticas.

Ensina Schellenberg (2006, p. 82) que essa função arquivística é a base para uma administração eficiente de documentos correntes e que “todos os outros aspectos de um programa que vise ao controle de documentos dependem da classificação”. Com a classificação, é possível compreender a dinâmica documental a partir de uma visão geral do âmbito em que o documento arquivístico é produzido, pois tornam-se claros os vínculos que o documento possui com o órgão ou entidade produtora. Essa visão ampla de todo o processo propicia, ainda, uma melhor compreensão do conteúdo do documento, o que é fundamental para a avaliação:

Sem a classificação, fica nebulosa a característica que torna os documentos de arquivo peculiares e diferenciados em relação aos demais documentos: a organicidade. Nenhum documento de arquivo pode ser plenamente compreendido isoladamente e fora dos quadros gerais de sua produção - ou, expresso de outra forma, sem o estabelecimento de seus vínculos orgânicos. Por consequência, a classificação torna-se condição para a compreensão plena dos documentos de arquivo – tanto a perspectiva de quem os organiza como de quem os consulta (GONÇALVES, 1998, p. 13, grifo da autora).

A eliminação de documentos sem critérios é um problema grave, que provoca grandes e irrecuperáveis lacunas em conjuntos documentais. Tão pernicioso quanto é a tendência de tudo guardar indiscriminadamente. Após a explosão documental, manter arquivados todos os documentos produzidos tornou-se

uma empresa impossível. Assim, a função arquivística avaliação assume papel central e decisivo para os objetivos da gestão racional dos documentos. Resume Arreguy:

De uma forma geral, entende-se avaliação como um processo de análise e seleção de documentos, tendo em vistas seus valores para a administração que o criou, para o cidadão em busca de seus direitos e para o pesquisador das mais diversas áreas, com o objetivo de determinar seu prazo de guarda e sua destinação final (ARREGUY, 2016, p. 49).

Arreguy (2016) reforça que avaliar é valorar. Portanto, trata-se de um ato que deve ser feito com critérios o menos subjetivo possível. A autora destaca que a redução da subjetividade é um objetivo que deve ser buscado. No entanto, pondera: “tem-se a consciência de ser algo intangível, especialmente no que diz respeito à determinação do valor informativo, dimensão do valor secundário, em que o nível de subjetividade pode chegar a graus bastante elevados” (ARREGUY, 2016, p. 49).

A subjetividade é uma das razões para que se recomende a formação de equipes com profissionais de áreas diferentes. Em sua proposta de conceituação, Bernardes acrescenta a interdisciplinaridade como elemento que caracteriza esta função:

Trabalho interdisciplinar que consiste em identificar valores para os documentos (imediate e mediato) e analisar seu ciclo de vida, com vistas a estabelecer prazos para sua guarda ou eliminação, contribuindo para a racionalização dos arquivos e eficiência administrativa, bem como para a preservação do patrimônio documental (BERNARDES, 1998, p. 14).

Outro aspecto a se considerar é a necessidade de fazer a avaliação no momento de produção do documento. Paes (1987) entende que os arquivos correntes são o calcanhar de aquiles da Arquivologia. Para a autora, com a criação de inúmeros “projetos-memória”, àquela época, os arquivos permanentes recebiam mais atenção e recursos em detrimento dos correntes. Apesar da maior disponibilidade de recursos (técnico-científicos, normatização e profissionais) para atacar o problema, a realidade atual não difere muito, pois não há na maioria das instituições a existência de uma cultura arquivística. Uma das consequências da pouca atenção dada aos arquivos correntes é a formação de massas documentais acumuladas. Indolfo recomenda:

Deve evitar-se a transferência para os arquivos intermediários de documentos que não tenham sido, anteriormente, avaliados, pois, o desenvolvimento do processo de avaliação e seleção nestes arquivos tem se mostrado extremamente oneroso do ponto de vista técnico e gerencial, bem como tem levado a formação de massas documentais volumosas, descaracterizando a função primordial dos arquivos de apoio às atividades gerenciais (INDOLFO, 2007, p. 43).

Dessa forma, a aplicação de critérios de avaliação já na criação dos documentos permitirá a distinção de documentos com valor informativo ou probatório daqueles destituídos de quaisquer valores. No entender de Bernardes (1998, p. 14), “a avaliação deverá ser realizada no momento da produção, paralelamente ao trabalho de classificação, para evitar a acumulação desordenada, segundo critérios temáticos, numéricos ou cronológicos”. Partilhando da mesma opinião, Indolfo assevera de forma contundente:

A prática de promover a avaliação em outra idade, que não seja a corrente, é considerada totalmente inadequada, pois os acervos acumulados encontram-se descontextualizados, na maioria das vezes, não classificados, apresentando características que exigirão propostas de destinação acompanhadas de justificativas específicas (INDOLFO, 2007, p. 47, grifo nosso).

O produto do processo de avaliação é a tabela de temporalidade que deve ser utilizada em associação com o Plano de Classificação. Para Dingwall (2016, p. 211), esses instrumentos são a “materialização do modelo do ciclo vital de uma entidade em particular”. A tabela de temporalidade é...

[...] o instrumento fundamental da avaliação, pois ela registra o ciclo de vida dos documentos. Nela devem constar os prazos de arquivamento dos documentos no arquivo corrente, de sua transferência ao arquivo central ou intermediário, e de sua destinação final, quando se determina sua eliminação ou recolhimento ao arquivo permanente (BERNARDES, 1998, p. 21).

A tabela de temporalidade, depois de elaborada, deve ser submetida à aprovação de instituição arquivística competente da esfera governamental à qual o órgão ou entidade pertença. Sua efetiva utilização deverá ser orientada por uma Comissão Permanente de Avaliação de Documentos (CPAD), composta





## **Criptografia**

Criptografia é um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de “tradução” da mensagem. Nas comunicações digitais, a criptografia auxilia na proteção de todos os conteúdos transmitidos entre duas ou mais fontes, evitando a interceptação por parte de cibercriminosos, hackers e espões, por exemplo.

Atualmente, a maioria dos sites na internet utilizam comunicações criptografadas, principalmente em locais onde dados bancários, passwords e arquivos pessoais estejam armazenados.

Além de prevenir que pessoas não-autorizadas tenham acesso aos dados e informações trocadas na rede online, a criptografia também impede que backups sejam acessados por usuários indevidos.

Etimologicamente, o termo “criptografia” se originou a partir do grego, formado pela união dos elementos *kryptós*, que significa “secreto” ou “oculto”, e *graphía*, que quer dizer “escrita”. Assim, o significado literal de criptografia é “escrita secreta”.

No cotidiano, sistemas de criptografia são utilizadas pelos usuários de aplicativos e softwares de troca de mensagens instantâneas, como o Whatsapp, por exemplo.

## **Tipos de Criptografia**

Nas comunicações feitas através de dispositivos eletrônicos, o método mais utilizado de criptografia são as chamadas “chaves criptográficas”.

As chaves criptográficas consistem em conjuntos de algoritmos que codificam uma mensagem publicamente legível em um texto cifrado, ou seja, composto por valores secretos que só podem ser decifrados com o código de acesso correto.

Existem dois principais tipos de chaves criptográficas, estudadas através do ramo da Matemática conhecido por Criptologia: as simétricas e as assimétricas.

### **Simétrica**

Também conhecida por “criptografia de chave única” ou “criptografia de chave privada”, este modelo utiliza apenas um conjunto de algoritmos responsáveis tanto pela cifragem de determinada operação, assim como a sua decifragem.

Neste caso, o pressuposto da confiabilidade entre os interlocutores deve ser total, visto que ambos partilham de uma única chave de criptografia, tanto para codificar como para decodificar uma mensagem, por exemplo.

### **Assimétrica**

Também conhecido como “criptografia de chave pública”, este é um sistema de protocolos criptográficos que requer a formação de duas chaves, sendo uma privada (usada para decodificar) e a outra pública (utilizada para codificar e autenticar assinaturas digitais, por exemplo).

Com a criptografia assimétrica, qualquer pessoa pode enviar uma mensagem criptografada usando a chave pública, mas apenas os receptores com a chave privada conseguem decodificá-la. O segredo da informação consiste em manter em sigilo o código da chave privada, por exemplo.

Em linhas gerais, criptografia é o nome que se dá a técnicas que transformam informação inteligível em algo que um agente externo seja incapaz de compreender. De forma mais simples, a criptografia funciona como códigos: sem ela, um criminoso poderia interceptar a sua senha de e-mail durante o login.

Com a criptografia, caso ele intercepte seu acesso, mas não tenha a chave correta, verá apenas uma lista desordenada e aparentemente confusa de caracteres, que não leva a lugar nenhum.

A criptografia é um método de proteção e privacidade de dados muito importante e cada vez mais presente. Do ponto de vista prático para quem usa Internet e dispositivos que oferecem proteção criptográfica, há tipos ou termos, que é preciso conhecer: criptografia simétrica e assimétrica (ou de ponta a ponta).

### **Criptografia Simétrica**

O tipo de criptografia simétrica é o mais comum e pressupõe que uma mesma chave usada para ocultar informação precisa ser aplicada para revela-la na outra ponta. É o tipo de criptografia usada na época da Segunda Guerra Mundial, por exemplo, e protagonista da história da invenção do computador, como conhecemos hoje.

### **Criptografia Assimétrica ou de Ponta-a-Ponta**

Atualmente, os dois protocolos mais usados para proteção de dados na Internet, o SSL (Secure Sockets Layer) e o TLS (Transport Layer Security) utilizam a criptografia simétrica para proteger os dados transmitidos e armazenados.

No entanto, a criptografia simétrica possui um desafio conceitual importante e impossível de ser resolvido. Como combinar uma chave secreta entre duas pessoas que querem se comunicar através da Internet de forma que ela não possa ser obtida por um invasor? Essa pergunta não teve solução até a década de 1970.

A solução foi dada pela criptografia assimétrica, na qual utiliza-se duas chaves distintas, mas que se complementam. Por essa propriedade, dá-se o nome de par de chaves, que é composto pela chave pública e pela chave privada. A chave pública é liberada para todos que desejam se comunicar com o emissor da chave enquanto a chave privada fica em poder de quem a emitiu.

O algoritmo de criptografia mais usado atualmente é o RSA, denominado pelas iniciais dos seus criadores, Ronald Rivest, Adi Shamir e Leonard Adleman. Uma desvantagem dos algoritmos de criptografia assimétrica existentes é o seu desempenho, que são mais lentos que os métodos simétricos.

Sendo assim, na prática, a criptografia assimétrica é utilizada para definir uma chave de sessão, que será usada na criptografia simétrica durante a comunicação. Esse é o funcionamento dos protocolos SSL e TLS, usados largamente na Internet.

Na criptografia assimétrica, as chaves públicas podem ser forjadas, fazendo com que o emissor não obtenha a chave pública correta do destinatário. Para solucionar esse problema, os engenheiros da Internet criaram a figura da Autoridade Certificadora, que funciona como um cartório, autenticando as chaves públicas das pessoas.

É essa autenticação da chave pública do seu banco, por exemplo, que faz o seu navegador exibir o singelo cadeado de segurança, fazendo com que você saiba que o site é mesmo do banco e não de um criminoso.

Esses aplicativos de mensagens oferecem a criptografia de ponta-a-ponta, que pressupõe proteção de conteúdo das mensagens trocadas entre os usuários numa mecânica em que nem mesmo o próprio administrador dos aplicativos pode ler o conteúdo.

Ponta-a-ponta é um sinônimo para o tipo assimétrico, e no caso específico desses aplicativos, se refere ao fato de que cada usuário dentro dessas redes possui uma chave de criptografia específica que é combinada com a de seus contatos durante a troca de mensagens. Dessa forma, o conteúdo trocado entre duas pessoas pelos mensageiros só é visível por elas.

### **Criptografia no Computador e no Celular**

Ainda é muito comum associar o uso da criptografia diretamente com a proteção de dados na Internet: com a técnica, é muito mais difícil o criminoso descobrir seu login e senha de qualquer site e seus dados bancários são protegidos a cada compra.

Mas a criptografia tem aplicações que vão além disso. No computador, caso você decida criptografar seus dados, o windows ou macOS aplicarão uma chave criptográfica que protegerá todo o conteúdo

armazenado na máquina de forma que só se torne visível por quem possua a chave, no caso o seu PIN, senha de usuário na máquina, ou qualquer tipo de autenticação biométrica oferecida pelo Windows, por exemplo.

Para celulares android e iPhone (iOS) a mesma coisa é válida. Ao criptografar os dados no aparelho, você os torna essencialmente inacessíveis a um invasor.

### **Níveis de Segurança**

A criptografia depende da aplicação e do nível de segurança exigido, mas em linhas gerais, uma criptografia de 128 bits é muito mais segura do que uma de 56 bits, por exemplo.

Uma chave de 56 bits oferece 72 quadrilhões de possibilidades de troca de caracteres para ocultar uma mensagem (parece absurdo, mas computadores já podem fazer bilhões de operações por segundo, então 56 bits pode não ser tão seguro assim se o hacker possuir um aplicativo que tenta milhões de alternativas para quebrar a criptografia a cada segundo).

Para comparar, uma chave de 128 bits tem 339,000,000,000,000,000,000,000,000,000 de possibilidades (arredondando, há uns trilhões a mais)

### **Criptografia**

A criptografia é uma técnica utilizada há anos que com o passar do tempo evoluiu a ponto de oferecer soluções eficazes no que diz respeito à segurança da informação. Hoje, ela é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e consiste basicamente na transformação de determinado dado ou informação a fim de ocultar seu real significado.

Este artigo apresenta os conceitos sobre criptografia, seus tipos, aplicabilidade e como ela é empregada no .NET por meio do namespace System.Security.Cryptography. Ao final do artigo será desenvolvida uma aplicação para criptografar dados usando um algoritmo simétrico. Além disso, iremos criar uma DLL contendo a classe de criptografia implementada, que poderá ser reutilizada em outros projetos.

### **Em que Situação o Tema é Útil**

A criptografia pode ser utilizada em aplicações e ambientes cuja segurança das informações é algo relevante para o projeto, principalmente em sistemas WEB, onde o dado trafega em um meio público correndo um risco maior de ser interceptado, fato este que pode gerar prejuízos enormes para uma organização. O domínio das técnicas de criptografia não é algo complexo quando estamos trabalhando com o paradigma orientado a objetos, sendo essencial para a criação de aplicações seguras.

Há pouco tempo, quando a tecnologia ainda não era muito presente em nosso cotidiano, as informações e grande parte dos processos organizacionais eram geridos basicamente no papel, sendo armazenados em armários ou cofres protegidos por cadeados ou senhas.

Atualmente este paradigma mudou, pelo menos para uma parcela significativa da sociedade. As informações são processadas e armazenadas em meios digitais, criando uma forte dependência entre os sistemas de informação e as organizações. Com o advento da internet, os dados trafegam em meios públicos, podendo ser interceptado por qualquer um que esteja mal intencionado. Neste cenário, uma falha na segurança destes conteúdos pode acarretar em enormes prejuízos para uma corporação.

Então, o que fazer para garantir tal segurança? Existem diversos meios de proteção e um deles é o uso da criptografia. Ela não vai impedir que uma determinada informação seja interceptada, mas tem o objetivo de dificultar a compreensão do dado capturado. Mas como isso é feito? Há vários algoritmos de criptografia que cumprem este papel, cada um com suas particularidades, porém a ideia central é a mesma: modificar a informação de forma que apenas o destinatário consiga compreender a que foi transmitido.

Vale ressaltar que a criptografia não é aplicada apenas quando um dado é enviado de um local a outro, ela é utilizada também em dispositivos de armazenamento de dados (ex: discos rígidos, pen drives, storages), que são alvos de ataques e roubos. Ou seja, de uma forma geral, a criptografia vai garantir



a confidencialidade da informação. Nos próximos tópicos, veremos alguns conceitos relacionados a esta técnica.

### **Criptografia Simétrica**

A criptografia simétrica foi o primeiro tipo de criptografia criado. Os algoritmos que a utilizam têm como característica principal o uso de uma mesma chave criptográfica (Nota do DevMan 1) para criptografar ou descriptografar uma informação, por isso o adjetivo “simétrico” dá nome a esta técnica. Exemplificando um pouco este conceito, quando um emissor cifra uma mensagem com um algoritmo de criptografia simétrico, ele utiliza uma chave, que é representada por uma senha ou um conjunto de bits para codificar os dados. O receptor então faz uso do algoritmo para descriptografar a mensagem e aplica a mesma chave que foi utilizada pelo emissor para voltar à mensagem em sua forma original. Sem a mesma, não é possível decifrar a informação recebida.

#### **Nota do DevMan 1**

Chave criptográfica é um conjunto de caracteres formando uma sequência de bits que trabalhando em conjunto com um algoritmo de criptografia irão determinar o resultado final do processo de cifragem e decifragem da mensagem. O nível de segurança da codificação depende tanto do algoritmo quanto do tamanho da chave escolhida (total de bits que ela possui).

Uma forma muito utilizada por invasores para descobrir esta chave é utilizando a força bruta, onde são utilizadas inúmeras combinações de caracteres na tentativa de uma delas ser a chave do algoritmo. Veja na Figura 1 o processo de criptografia simétrica. Observe que a mesma chave é utilizada nos algoritmos para cifragem e decifragem do texto.

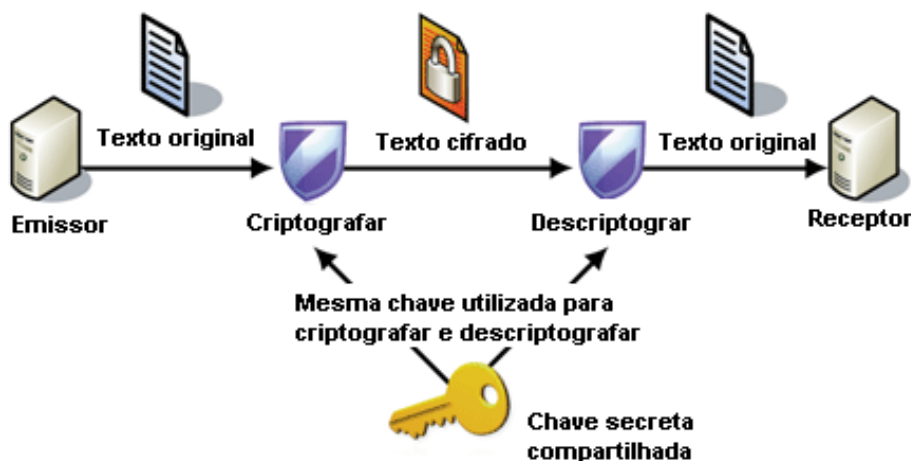


Figura 1. Processo de criptografia simétrica.

Como vantagens deste método podemos citar a simplicidade na sua implementação, uma vez que é utilizada uma única chave no processo de cifragem e decifragem do dado, além da velocidade deste processo em relação à criptografia assimétrica, que veremos nos próximos tópicos, possibilitando assim que uma grande quantidade de dados seja encriptada em pouco tempo.

Por outro lado este modelo de criptografia apresenta algumas falhas que estão relacionadas à geração e compartilhamento das chaves: no primeiro caso uma chave muito simples pode ser facilmente quebrada utilizando um algoritmo de força bruta.

Já na segunda situação deve-se atentar para a forma como as chaves são compartilhadas entre os interessados na informação, a fim de evitar que a mesma seja obtida por um invasor.

Alguns algoritmos de criptografia simétrica bem conhecidos são: DES (Data Encryption Standart), Triple DES, AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, RC4.

### **Criptografia Assimétrica**

A criptografia assimétrica, também denominada como criptografia de chave pública, possui como característica básica o uso de duas chaves ao invés de uma, sendo elas:

Chave pública: Chave que pode ser distribuída para outros usuários.

Chave privada. Chave que deve ser mantida em segredo.

A criptografia diz respeito a conceitos e técnicas usadas para codificar uma informação, de tal forma que somente seu real destinatário e o emissor da mensagem possam acessá-la, com o objetivo de evitar que terceiros interceptem e entendam a mensagem.

Atualmente, as técnicas de criptografia mais conhecidas envolvem o conceito das chaves criptográficas, que são um conjunto de bits, baseados em um algoritmo capaz de interpretar a informação, ou seja, capaz de codificar e decodificar. Se a chave do receptor não for compatível com a do emissor, a informação então não será extraída.

O termo criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Existem dois tipos de chave: a chave pública e a chave privada.

A chave pública é usada para codificar as informações, e a chave privada é usada para decodificar. Assim, na pública, todos têm acesso, mas para 'abrir' os dados da informação, que aparentemente são sem sentido, é preciso da chave privada, que só o emissor e receptor originais têm.

Atualmente, a criptografia pode ser considerada um método 100% seguro, ou seja, quem a utiliza para mandar e-mails e proteger seus arquivos, estará protegido contra fraudes e tentativas de invasão.

Os termos 'chave de 64 bits' e 'chave de 128 bits' são usados para expressar o tamanho da chave, assim, quanto mais bits forem utilizados, mais segura será essa criptografia. Um exemplo disso é se um algoritmo usa uma chave de 8 bits, por exemplo, apenas 256 chaves poderão ser utilizadas para decodificar essa informação, porque 2 elevado a 8 é igual a 256. Assim, um terceiro pode tentar gerar 256 tentativas de combinações e decodificar a mensagem, que mesmo sendo uma tarefa difícil, não é impossível. Por isso, quanto maior o número de bits, mais segura será a criptografia.

Existem dois tipos de chaves criptográficas, as chaves simétricas e as chaves assimétricas.

### **Chave Simétrica**

É um tipo de chave simples, que é usada para a codificação e decodificação. Entre os algoritmos que usam essa chave, estão:

DES (Data Encryption Standard): Faz uso de chaves de 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações. Mesmo sendo um número absurdamente alto, em 1997, conseguiram quebrar esse algoritmo através do método de 'tentativa e erro', em um desafio na internet.

RC (Ron's Code ou Rivest Cipher): É um algoritmo muito utilizado em e-mails e usa chaves de 8 a 1024 bits, além de possuir várias versões que se diferem uma das outras pelo tamanho das chaves.

EAS (Advanced Encryption Standard): Hoje em dia é um dos melhores e mais populares algoritmo de criptografia existente. Você pode definir o tamanho da chave como sendo de 128bits, 192bits ou 256bits.

IDEA (International Data Encryption Algorithm): É um algoritmo que usa chaves de 128 bits, parecido com o DES. Seu ponto forte é a fácil implementação de software.

As chaves simétricas não são totalmente seguras quando se trata de informações muito valiosas, principalmente pelo fato de que o emissor e o receptor têm que conhecer a mesma chave. Assim, a transmissão pode não ser segura e o conteúdo chegar a terceiros.

### **Chave Assimétrica**

A chave assimétrica utiliza duas chaves: a privada e a pública. Elas se resumem da seguinte forma: a chave pública para codificar e a chave privada para decodificar, levando-se em consideração que a chave privada é secreta.

Entre os algoritmos utilizados, estão:

RSA (Rivest, Shamir and Adleman): É um dos algoritmos de chave assimétrica mais utilizados, em que dois números primos (aqueles que só podem ser divididos por 1 e por eles mesmos) são multiplicados para a obtenção de um terceiro valor. Para isso, é preciso fazer fatoraçoão, que é descobrir os dois primeiros números a partir do terceiro, que é um cálculo trabalhoso. Assim, se números grandes forem utilizados, será praticamente impossível descobrir o código. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido.

O termo criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la.

Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Os primeiros métodos criptográficos existentes usavam apenas um algoritmo de codificação. Assim, bastava que o receptor da informação conhecesse esse algoritmo para poder extraí-la. No entanto, se um intruso tivesse posse desse algoritmo, também poderia efetuar um processo de decifragem, caso capturasse os dados criptografados.

Há ainda outro problema: imagine que a pessoa A tivesse que enviar uma informação criptografada à pessoa B. Esta última teria que conhecer o algoritmo usado. Imagine agora que uma pessoa C também precisasse receber uma informação da pessoa A, porém a pessoa C não poderia descobrir qual é a informação a ser enviada à pessoa B. Se a pessoa C capturasse a informação enviada à pessoa B, também conseguiria decifrá-la, pois quando a pessoa A enviou sua informação, a pessoa C também teve que conhecer o algoritmo usado. Para a pessoa A evitar esse problema, a única solução seria utilizar um algoritmo diferente para cada receptor.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Você já deve ter ouvido falar de chave de 64 bits, chave de 128 bits e assim por diante. Esses valores expressam o tamanho de uma determinada chave. Quanto mais bits forem utilizados, mais segura será a criptografia. Explica-se: caso um algoritmo use chaves de 8 bits, por exemplo, apenas 256 chaves poderão ser usadas na decodificação, pois 2 elevado a 8 é 256.

Isso deixa claro que 8 bits é inseguro, pois até uma pessoa é capaz de gerar as 256 combinações (embora demore), imagine então um computador!

Porém, se forem usados 128 ou mais bits para chaves (faça 2 elevado a 128 para ver o que acontece), teremos uma quantidade extremamente grande de combinações, deixando a informação criptografada bem mais segura.

### **Chaves Simétricas e Assimétricas**

Há dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas. Ambas são abordadas a seguir:

### Chave Simétrica

Esse é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação. Existem vários algoritmos que usam chaves simétricas, como o DES, o IDEA, e o RC:

- DES (Data Encryption Standard): criado pela IBM em 1977, faz uso de chaves de 56 bits. Isso corresponde a 72 quatrilhões de combinações. É um valor absurdamente alto, mas não para um computador potente. Em 1997, esse algoritmo foi quebrado por técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet;

- IDEA (International Data Encryption Algorithm): criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES. Sua implementação em software é mais fácil do que a implementação deste último;

- RC (Ron's Code ou Rivest Cipher): criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6. Essencialmente, cada versão difere da outra por trabalhar com chaves maiores.

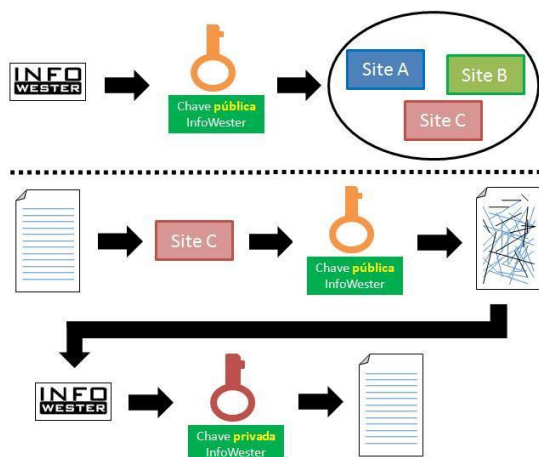
Há ainda outros algoritmos conhecidos, como o AES (Advanced Encryption Standard) - que é baseado no DES -, o 3DES, o Twofish e sua variante Blowfish, entre outros.

O uso de chaves simétricas tem algumas desvantagens, fazendo com que sua utilização não seja adequada em situações onde a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas ou entidades estejam envolvidas. Ainda, há o fato de que tanto o emissor quanto o receptor precisam conhecer a mesma chave. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas".

### Chave Assimétrica

Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma denominada privada e outra denominada pública. Neste método, um emissor deve criar uma chave de codificação e enviá-la ao receptor. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta.

Para melhor compreensão, imagine o seguinte: O InfoWester criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao InfoWester deverá utilizar a chave pública deste. Quando o InfoWester receber essa informação, apenas será possível extraí-la com o uso da chave privada, que só o InfoWester tem. Caso o InfoWester queira enviar uma informação criptografada a outro site, deverá obter uma chave pública fornecida por este.



Entre os algoritmos que usam chaves assimétricas, têm-se o RSA (o mais conhecido) e o Diffie-Hellman:



RSA (Rivest, Shamir and Adleman): criado em 1977 por Ron Rivest, Adi Shamir e Len Adleman nos laboratórios do MIT (Massachusetts Institute of Technology), é um dos algoritmos de chave assimétrica mais usados. Nele, números primos (número primo é aquele que só pode ser dividido por 1 e por ele mesmo) são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor.

Porém, descobrir os dois primeiros números a partir do terceiro (ou seja, fazer uma fatoração) é muito trabalhoso. Se dois números primos grandes (realmente grandes) forem usados na multiplicação, será necessário usar muito processamento para descobri-los, tornando essa tarefa praticamente inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido;

ElGamal: criado por Taher ElGamal, esse algoritmo faz uso de um problema matemático conhecido por "logaritmo discreto" para se tornar seguro. Sua utilização é freqüente em

Existem ainda outros algoritmos, como o DSA (Digital Signature Algorithm), o Schnorr (praticamente usado apenas em assinaturas digitais) e Diffie-Hellman.

### **Certificação Digital**

Um recurso conhecido por certificação digital é muito utilizado com chaves públicas. Trata-se de um meio que permite, por exemplo, provar que um certo documento eletrônico foi mesmo emitido por uma determinada entidade ou pessoa. O receptor da informação usará a chave pública fornecida pelo emissor para se certificar da origem. Além disso, a chave fica integrada ao documento de forma que qualquer alteração por terceiros imediatamente a invalide.

Criptografia (do grego kryptos, oculto, e graphein, escrever) é o nome dado a um conjunto de regras que visa codificar a informação de maneira que só o emissor e o receptor consiga decifrá-la.

A troca de informações sigilosas é uma prática antiga, existente há centenas de anos, e que até bem pouco tempo era predominante em meio aos livros e documentos. O surgimento da internet e a facilidade que esta proporciona de transmitir dados de maneira precisa e extremamente rápida fez de tal prática um recurso essencial para permitir que apenas emissor e receptor obtenham acesso livre à informação tratada.

A criptografia segue quatro princípios básicos: confidencialidade, autenticação, integridade da informação e não repudiabilidade (ou seja, o remetente não pode negar o envio da informação). Apesar de ser recurso importante na transmissão de informações pela internet, a criptografia não é capaz de garantir total segurança, pois sempre existe alguém que consegue desenvolver uma maneira de "quebrar" o código. Assim, as técnicas são constantemente aperfeiçoadas e tantas outras são criadas, como por exemplo a "criptografia quântica".

A primeira técnica utilizava apenas um algoritmo de decodificação. Assim, bastava o receptor do algoritmo para decifrá-la, mas caso um intruso conhecesse esse mesmo algoritmo, ele poderia decifrar a informações se interceptasse os dados criptografados. Hoje, entre as técnicas mais conhecidas há o conceito de chaves, ou então chaves criptográficas, no qual um conjunto de bits baseado em um determinado algoritmo é capaz de codificar e de decodificar informações.

Há dois tipos de chaves, a simétrica e a assimétrica, ou chave pública. Caso o receptor da mensagem resolva usar uma chave incompatível com a chave do emissor, a informação não será compartilhada. Há ainda outros conceitos envolvidos na área da criptografia, como a Função Hashing, usada em assinaturas digitais para garantir integridade, e as aplicações, como a certificação digital.

O avanço das técnicas de invasão e interceptação de dados forçou a consequente evolução da criptografia, que adotou codificações de 256, 512 e até 1024 bits. Isso significa que são geradas 21024 combinações diferentes de chaves para cada mensagem enviada, sendo que apenas uma é correta, de conhecimento apenas do emissor e do receptor.

Com a intenção de ajudar na defesa da liberdade individual nos Estados Unidos e no mundo inteiro, Philip Zimmermann desenvolveu o PGP (Pretty Good Privacy) em 1991. Disponibilizado gratuitamente, o PGP se tornou um dos meios de criptografia mais conhecidos, principalmente na troca de e-mails, utilizando chaves assimétricas. O software pode realizar também um segundo tipo de criptografia através de uma "chave de sessão" método que representa um tipo de chave simétrica.



## REFERÊNCIAS

Os links citados abaixo servem apenas como referência. Nos termos da lei brasileira (lei no 9.610/98, art. 8º), não possuem proteção de direitos de autor: As ideias, procedimentos normativos, sistemas, métodos, projetos ou conceitos matemáticos como tais; Os esquemas, planos ou regras para realizar atos mentais, jogos ou negócios; Os formulários em branco para serem preenchidos por qualquer tipo de informação, científica ou não, e suas instruções; Os textos de tratados ou convenções, leis, decretos, regulamentos, decisões judiciais e demais atos oficiais; As informações de uso comum tais como calendários, agendas, cadastros ou legendas; Os nomes e títulos isolados; O aproveitamento industrial ou comercial das ideias contidas nas obras.

Caso não concorde com algum item do material entre em contato com a Domina Concursos para que seja feita uma análise e retificação se necessário

A Domina Concursos não possui vínculo com nenhuma banca de concursos, muito menos garante a vaga ou inscrição do candidato em concurso. O material é apenas um preparatório, é de responsabilidade do candidato estar atento aos prazos dos concursos.

A Domina Concursos reserva-se o direito de efetuar apenas uma devolução parcial do conteúdo, tendo em vista que as apostilas são digitais, isso, [e, não há como efetuar devolução do material.

***A Domina Concursos se preocupa com a qualidade do material, por isso todo conteúdo é revisado por profissionais especializados antes de ser publicado.***





Prezado cliente,

É com imensa satisfação que expressamos nossa profunda gratidão pela sua escolha em adquirir suas apostilas de estudos conosco. A preferência pelo nosso serviço é motivo de grande alegria e reforça nosso compromisso em fornecer materiais de alta qualidade para contribuir efetivamente em seu caminho educacional.


Aqui na nossa loja, dedicamo-nos diariamente para oferecer produtos que atendam não apenas às suas necessidades de aprendizado, mas que também superem suas expectativas. Cada compra realizada é um voto de confiança em nossa equipe, e estamos comprometidos em corresponder a essa confiança através de excelência em produtos e atendimento.

Saiba que sua decisão de confiar em nós para sua jornada de estudos é valorizada e respeitada. Estamos sempre empenhados em aprimorar nossos serviços para garantir que sua experiência seja positiva e produtiva. Se houver algo específico que possamos fazer para melhor atendê-lo, por favor, não hesite em nos informar.

Agradecemos por fazer parte da nossa comunidade de clientes e por escolher a qualidade e confiabilidade das nossas apostilas. Estamos ansiosos para continuar a servi-lo com dedicação e comprometimento.

Atenciosamente, Domina Concursos.

 [contato@dominaconcursos.com.br](mailto:contato@dominaconcursos.com.br)

 WhatsApp (48) 9.9695-9070



Rua Aracatuba, nº 45,  
Centro, Criciúma/SC - CEP  
88810-230