**POLÍCIA MILITAR DO DISTRITO FEDERAL**

**INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS**

# SINAIS IDENTIFICADORES DE AUTENTICAÇÃO: SOLUÇÃO DE PROTEÇÃO DE DADOS NA CORPORAÇÃO

Autor: CAD PM Bruno Moreira Costa
Orientador: Maj Publio Pastrolin Cavalcante

Brasília/DF

2021

**BRUNO MOREIRA COSTA**

# SINAIS IDENTIFICADORES DE AUTENTICAÇÃO: SOLUÇÃO DE PROTEÇÃO DE DADOS NA CORPORAÇÃO

Trabalho de conclusão de curso apresentado ao curso de graduação em Ciências Policiais do Instituto Superior de Ciências Policiais, como requisito parcial para aprovação na disciplina de Trabalho de Conclusão de Curso II.

Major Públio Pastrolin Cavalcante

:

Brasília/DF

2021

**BRUNO MOREIRA COSTA**

# SINAIS IDENTIFICADORES DE AUTENTICAÇÃO: SOLUÇÃO DE PROTEÇÃO DE DADOS NA CORPORAÇÃO

Trabalho de conclusão de curso apresentado ao curso de graduação em Ciências Policiais do Instituto Superior de Ciências Policiais, como requisito parcial para aprovação na disciplina de Trabalho de Conclusão de Curso II.

Brasília/DF

2021

**BANCA EXAMINADORA**

_____

Professor Orientador:  Me. Públio Pastrolin Cavalcante (Major PMDF)

_____

Professor Coorientador:  Me. Paulo Henrique Ferreira Alves (Major PMDF)

_____

Examinador Externo: Esp.Wellington da Costa Lange (Capitão PMDF)

## AGRADECIMENTOS


> “Mais importante do que a guerra, é quem está do seu lado na trincheira.”

A Deus pela sua infinita misericórdia e por me abençoar na trajetória dessa formação.

Ao Centro de Inteligência da PMDF nas pessoas do meu orientador, Major Pastrolin e do Sargento Anderson Cerqueira, camaradas desde a época do Departamento de Controle e Correição.

Pelo grande apoio do amigo Cadete Bentmuller.

Minha gratidão.

# SINAIS IDENTIFICADORES DE AUTENTICAÇÃO: SOLUÇÃO DE PROTEÇÃO DE DADOS NA CORPORAÇÃO

BRUNO MOREIRA COSTA

## RESUMO

A informação é cada vez mais o o ativo mais importante das instituições privadas e sobretudo públicas. A produção diária de dados pela Policia Militar do Distrito Federal em seu serviço fim requer uma atenção especial dado ao grande valor estratégico de um banco de dados formado por informações pessoais e especialmente por ser operado por diversos usuários. Desse modo, vulnerabilidades devem ser identificadas e antecipadas. Portanto, é extremamente relevante a composição de diversos mecanismos de proteção de dados, tal como o produto proposto pelo presente trabalho, por meio de um sinal identificador único para cada Policial Militar.

**Palavras-chave**: Segurança da Informação. Proteção de dados. Vulnerabilidades.

# AUTHENTICATION IDENTIFYING SIGNS: DATA PROTECTION SOLUTION AT THE CORPORATION

BRUNO MOREIRA COSTA

## ABSTRACT

Information has become the most important asset of private and, above all, public institutions. The daily production of data by the Military Police of the Federal District in its core role requires special attention given the strategical value of a database formed by private information and especially since it is operated by several users. In this context, vulnerabilities must be identified and anticipated. Therefore, the composition of several data protection mechanisms is extremely relevant, as the proposed product of this work, through a unique identifier signal for each Military Police officer.

**Keywords**: Information Security. Data protection. Vulnerabilities.

**SUMÁRIO**

## 1 INTRODUÇÃO

No âmbito da Polícia Militar do Distrito Federal (PMDF), um dos principais instrumentos utilizados por seus membros nas atividades típicas é o sistema Gênesis. Tal sistema foi instituído pela portaria PMDF nº 1019, de 30 de setembro de 2016, como pode-se verificar em seu artigo 2º:

> Art. 2º O Sistema Gênesis é um sistema informacional computadorizado que apresenta um conjunto de elementos inter-relacionados para coleta, cadastro, armazenamento, distribuição e processamento de dados relacionados ao gerenciamento operacional e aos atendimentos policiais operacionais (ações, operações, ocorrências e outras atividades policiais operacionais) realizados pela Polícia Militar do Distrito Federal, com a finalidade de facilitar o planejamento, controle, coordenação, análise e o processo decisório nos níveis operacionais, tático e estratégico da Corporação.

Atualmente, o acesso ao sistema é realizado por meio de *login* e senha informados pelo usuário, isto é, policial militar, o qual é empregado para consultas ao banco de dados e eventuais registros inerentes ao serviço policial militar. O detalhamento desse acesso está contido no artigo 5º da portaria PMDF nº 1019/2016, o qual dispõe que

> Art. 5º O acesso ao Sistema Gênesis dar-se-á através da *intranet* da PMDF ao efetivo da ativa, classificado e exercendo função na PMDF, sendo que o nível de acesso a cada módulo será de acordo com a lotação, a função do policial militar e a necessidade de conhecer, considerando-se a natureza do serviço executado e demais normas e legislações pertinentes.
> Parágrafo único. Solicitações de acesso ao Sistema Gênesis e/ou a seus bancos de dados por parte de outros órgãos públicos será objeto de análise pelo Estado Maior e Centro de Inteligência, observando-se critérios legais e técnicos e, se for o caso, concedido exclusivamente através de lavratura do devido documento legal assinado por ambos os órgãos.

Chama-se atenção o fato de que após o simples ingresso no sistema – por intermédio de qualquer computador ou *smartphone* e sem que haja identificação do policial militar que realizou o *login* – seja possível a obtenção, captura e arquivamento de dados. Isto é, telas que contenham dados de pesquisa quer seja de pessoas, de placa de veículos, de registros de atendimento policial, de imagens, de escalas de

serviços quer seja dos demais dados pertinentes ao serviço operacional sejam impressos, fotografados ou arquivados na forma de *print*, de captura de tela.

Pode-se identificar, deste modo, possível vulnerabilidade na base de dados do sistema Gênesis, a qual é diariamente alimentada ininterruptamente pelo serviço policial militar. Ressalta-se que a portaria retromencionada determinou, nos seus artigos 21 e 23, a restrição de acesso e de sua finalidade, bem como responsabilização do agente no caso de descumprimento de seus termos. Confira-se, *ipsis litteris*:

> Art. 21. Os dados inseridos no Sistema Gênesis são de acesso restrito à atividade policial militar, sendo que seu acesso e sua divulgação deverá ocorrer atendendo, exclusivamente, às normas internas da PMDF para divulgação de dados e em conformidade com as leis vigentes.
> [...]
> Art. 23. O descumprimento da presente Portaria poderá ensejar responsabilização disciplinar, criminal militar, e/ou outras previstas no ordenamento jurídico.

A despeito das previsões normativas quanto à restrição de acesso e à divulgação dos dados do Gênesis, bem como à imputação de responsabilidade no caso de descumprimento, infelizmente ainda não há ferramenta de segurança da informação que permita a sua efetividade. Ou seja, o sistema Gênesis apresenta uma falha na segurança, uma brecha, um problema para o qual sua resolução é relevante à PMDF.

Diante desse problema, a pesquisa aqui proposta pretende responder a três perguntas-problemas:

i. A PMDF consegue identificar e individualizar eventual vazamento de dados do sistema Gênesis?;
ii. Diante de um *print*, impressão e/ou foto do sistema Gênesis, a PMDF identificaria o seu responsável?;
iii. Qual é a importância da implementação de ferramentas de segurança da informação em caso de vazamento de dados do sistema Gênesis?.

Com vistas a responder a tais questionamentos, deve-se ressaltar que esta pesquisa é norteada pela segurança da informação e pela proteção. Espera-se que

ao final desta pesquisa seja possível fornecer, enquanto produto, uma identificação única a cada Policial Militar da corporação, permitindo assim que o Centro de Inteligência da PMDF esteja apto a identificar o responsável pelo vazamento de dados por intermédio de *prints,* impressão e/ou foto do sistema Gênesis, bem como a consequente má utilização de informação.

## 2 HIPÓTESES

Alicerçado no contexto-problema apresentado, é possível elencar as seguintes hipóteses:

i. a PMDF não consegue identificar e individualizar eventual vazamento de dados do sistema Gênesis; e
ii. diante de um *print*, impressão e/ou foto do sistema Gênesis, a PMDF não consegue identificar o seu responsável.

## 3 JUSTIFICATIVA E ESTADO DO CONHECIMENTO

Inicialmente, deve-se ressaltar que a práxis profissional instigou a investigação das perguntas-problema aqui propostas. A experiência relacionada à apuração de crimes e de transgressões disciplinares no âmbito do Departamento de Controle e Correição da PMDF permitiu identificar que uma das dificuldades do cotidiano das investigações consistia nos obstáculos técnicos para a identificação e consequente responsabilização do agente pelo mau uso ou pela disponibilização indevida de informações através de meios eletrônicos.

Com base nesse contexto, foi identificada uma possível vulnerabilidade dos sistemas da PMDF, notadamente do Gênesis, que é o mais utilizado no contexto do serviço policial militar. Vale ressaltar, no entanto, que, na alçada institucional, a preocupação com a segurança das informações existentes em bancos de dados da PMDF, cujo acesso é restrito, é crescente e necessária, bem como a discussão a respeito da melhor proteção dos seus dados.

No que concerne ao tema da segurança da informação, é preciso salientar que se trata de “[...] área do conhecimento que ainda apresenta muitas lacunas, inclusive de estudos específicos sob a ótica do setor público” (NOBRE; RAMOS; NASCIMENTO, 2010, s. p.). Além disso, cada vez mais, a informação se torna o bem ou o conjunto de bens mais importante em todos os segmentos, sejam privados, sejam públicos. Na esfera policial, representa ativo de valor imensurável na finalidade institucional de segurança pública, razão pela qual deve ser tratada e protegida adequadamente.

Segundo Ramos (2008, s. p.), “costuma-se proporcionar segurança a tudo aquilo que possui valor e, que, consequentemente, demanda proteção”. Ainda conforme este autor, a despeito da aplicação genérica a diversas áreas, “[...] quando o assunto é a informação, esse princípio também pode ser aplicado, porque toda informação que possui valor deve ser protegida.” (RAMOS, 2008, s. p.).

No que diz respeito ao valor da informação na sociedade e nas relações modernas, Brito (2011) acentua que os serviços prestados à sociedade devem ser realizados sem que haja exposição excessiva a riscos e/ou ameaças. Apesar disso, no que se refere à segurança das informações contidas no sistema Gênesis, devido às interações usuário/sistema, há uma falsa sensação de segurança, pois a informação não é dissociada do usuário, sendo tais informações a todo instante

manipuladas e o sistema, alimentado. Pode-se depreender, portanto, que, no contexto do sistema Gênesis, não se sabe a real dimensão do risco à segurança do sistema, consequentemente as medidas de proteção e segurança da informação podem ser ineficazes.

Deve-se enfatizar ainda que a interação do usuário com os dados contidos nos sistemas deve ser levada em consideração para que se possa falar em e discutir sobre segurança da informação. Por esse motivo, nada mais lógico, para este projeto e para a pesquisa em andamento, discorrer de conceitos referentes à segurança da informação, sendo apresentados por diferentes autores.

O conceito de segurança da informação pode ser compreendido de diferentes formas. Segundo para Zapater e Suzuki (2005, s. p.), a segurança da informação

> [...] pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associadas aos diversos ativos informacionais de uma corporação, independentemente da forma ou do meio em que são compartilhados ou armazenados.

Já conforme Summers (1997), a segurança da informação é uma "[...] componente conjugada ao uso de computadores e a considerou uma meta a ser atingida, para proteger os sistemas computacionais contra ameaças à confidencialidade, à integridade e à disponibilidade.". A seu turno, Sêmola (2003, s.p.), entender que esta "é uma área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, contra alterações indevidas ou contra sua indisponibilidade".

De acordo com Peltier (2001, p. 166),

> [...] segurança da informação compreende o uso de controles de acessos físicos e lógicos para os dados, a fim de garantir o uso apropriado desses dados e impedir modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou acesso aos registros e aos arquivos, de forma manual ou automaticamente, bem como perdas, danos ou mau uso dos ativos informacionais.

Já McDaniel (1994, p. 87) identifica que ela é composta "de conceitos, de técnicas e de medidas técnicas e administrativas usadas para proteger os ativos informacionais", não apenas de danos, mas de "revelação, manipulação, perda ou uso não autorizados, deliberada ou inadvertidamente".

Além dos pressupostos conceituais apresentados, o termo também recebeu definição no dicionário de biblioteconomia e arquivologia:

> [...] conjunto de procedimentos para a proteção do acervo informacional de uma organização contra acesso, ou uso por pessoas não autorizadas. Essa proteção é caracterizada pela preservação da: a) confiabilidade; b) integridade; c) disponibilidade. (CUNHA; CAVALCANTI, 2008, s. p.)

Por fim, acrescente-se que a ISO/IEC 27001 define como objetivo da segurança da informação a proteção das infraestruturas críticas e a viabilização de negócios, bem como evitar ou reduzir os riscos relevantes. Ademais, preceitua como objetivo:

> [...] a salvaguarda das informações para que não sejam manipuladas de forma indevida e a mitigação dos riscos que podem deixar a informação indisponível ou com perda de suas propriedades (Associação Brasileira de Normas Técnicas, 2013, s. p.).

No que se refere ao objetivo das ações de segurança da informação, Manoel (2014) indica a proteção das informações às ameaças, a fim de que a organização tenha garantida suas atividades, minimizem-se riscos e maximizem-se o retorno sobre os investimentos e as oportunidades de negócio (MANOEL, 2014).

A segurança da informação é identificada pelos atributos da confidencialidade, da integridade e da disponibilidade. Nos termos da Associação Brasileira de Normas Técnicas (2013, s. p.),

> [...] a integridade [...] se relaciona com a fidedignidade e totalidade da informação bem como sua validade; a disponibilidade [...] se relaciona com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro; e a confidencialidade [...] está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida.

De acordo com Siewert (2008, p. 89), a chamada *tríade CIA* orienta a análise, o planejamento e a implementação da segurança da informação e assim pode ser detalhada:

> [...] Confidencialidade: significa garantir o segredo das informações, liberando acesso somente às pessoas autorizadas; a perda deste

> atributo ocorre quando pessoas não autorizadas obtêm acesso às informações confidenciais;
> Integridade: significa garantir que a informação não foi alterada indevidamente, ou seja, devem-se manter as características originais impostas pelo proprietário da informação, mantendo o seu ciclo de vida (nascimento, manutenção e destruição);
> Disponibilidade: significa garantir a disponibilidade da informação, sempre que necessário às pessoas autorizadas.

Relativamente aos principais mecanismos de segurança, no presente estudo utilizar-se-á a classificação de controles proposta por Böger e Bodemüller (2007), para quem, controles administrativos “são as políticas de segurança”; controles físicos “são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura, garantindo a existência da informação, que a suporta”; e controles lógicos:

> [...] são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico. Exemplos disto são os mecanismos de criptografias, assinatura digital, mecanismos de certificação, controle de acesso, entre outros. (BÖGER; BODEMÜLLER, 2007, p. 62)

Pretende-se com este estudo desenvolver o atributo da confidencialidade aliado ao controle lógico sob os dados manipulados diariamente pelos usuários na relação usuário/dados em que o usuário é a vulnerabilidade apontada.

Assim, tendo em vista a formação e a ampliação do banco de dados da PMDF e a utilização do sistema Gênesis e considerando o grande valor estratégico agregado a um banco de informações seguro e protegido, propõe-se uma pesquisa cujo produto é a criação de um sinal identificador único para cada Policial Militar no momento em que ele(a) acesse dados do sistema Gênesis e que nele faça as suas consultas.

Vale ressaltar ainda que

> [...] os sistemas são concebidos com segurança de acesso e rastreamento das operações, conforme protocolo AAAS. Controla-se quem acessa o sistema (*accounting*), garante-se que seja realmente quem se declara ser (*authentication*), que execute somente operações que possa executar (*authorization*) e que proteja a comunicação emissor/receptor (*secure transport protocol*). (IETF, 2017).

Dentre os objetivos da segurança da informação, a *Information Systems Audit and Control Association* (ISACA, 2012), ressalta a proteção das informações contra divulgação não autorizada.

Nesse sentido, a vulnerabilidade que aqui se ressalta é a interação usuário/ dados em que o elemento humano interfere diretamente no gerenciamento da segurança da informação, sendo desse modo uma vulnerabilidade crítica.

Nos termos concebidos por Sveen, Torres e Sariegi (2009, s. p.), é necessário

> [...] contemplar, de forma integradora, os elementos “pessoas”, “processos” e “tecnologias” como variáveis que coexistem nas empresas e que precisam ser tratadas com equilíbrio e igualdade de condições no âmbito da gestão de segurança da informação.

Dessa forma, observa-se que as pessoas são elementos importantes na gestão de segurança da informação, mas ainda pospostos em relação às soluções nos processos e tecnologias. Colwill (2010, s. p.) pontua que

> [...] o excesso de confiança na tecnologia, sem a consideração de outros fatores também relevantes, pode levar a resultados desastrosos na gerência de ameaça interna à segurança muito importante: o elemento humano. Este elemento traz riscos à segurança da informação, uma vez que pessoas podem obter acesso legítimo a informações, conhecem a organização e sabem a localização de ativos valiosos.

Kraemer, Carayon e Clem (2009) contribuem para essa perspectiva, observando que os usuários não são necessariamente contrários a segurança, mas muitas vezes são incapazes de determinar as implicações de suas ações na segurança.

Segundo Santos (2011), a principal ameaça para qualquer segurança é o próprio ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema.

Alinhando-se às evidências científicas que asseguram a importância da proteção dos dados na e para as instituições públicas, o Tribunal de Contas da União, emitiu a seguinte recomendação expressa em um de seus acórdãos:

> 9.1.3 orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do

> negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso; [...]. (Acórdão nº 1.603/2008-TCU Plenário).

Estabelecidas as premissas conceituais e o Estado do Conhecimento desta pesquisa, é necessário ressaltar que ela se alinha ao cumprimento do objetivo institucional de garantia de proteção de informações necessárias à tomada de decisão na gestão da informação para integração dos dados do Sistema de Informações Policial Militar (SIPOM), com a implantação de sistema de controle de informações, inserindo conteúdo de segurança da informação.

Além disso, atende às iniciativas estratégicas de gestão de segurança da informação, implementação de órgãos de perícia na Corporação, que foi previsto como um dos objetivos do aprimoramento dos processos internos da PMDF à gestão da segurança da Informação, tal como proposto nos termos no Planejamento Estratégico 2011 – 2022:

> 5. OBJETIVO: OTIMIZAR O GERENCIAMENTO DAS INFORMAÇÕES DESTINADAS AOS PÚBLICOS INTERNO E EXTERNO. Contribui para o seguinte Objetivo do Plano Estratégico da PMDF: 10. OBJETIVO: GARANTIR AS INFORMAÇÕES NECESSÁRIAS À TOMADA DE DECISÃO.
>
> 5.5 - Estratégia: IMPLANTAR A GESTÃO DE SEGURANÇA. PMDF – 10.4.5. Iniciativa: Desenvolver e implantar projetos de governança corporativa, gestão de segurança da informação (ISO 27.000) e gestão de riscos (ISO 31.000). 5.5.1 - Iniciativa: Implantar Política de Segurança da Informação e de Ativos conforme normas ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002. 5.5.2 - Iniciativa: Implantar o Sistema de Gestão de Segurança da Informação (normas ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002) / Política de Segurança da Informação e de Ativos, Plano de Continuidade de Negócios (norma ABNT NBR 22.301), Gestão de Riscos (ABNT ISO/IEC 31000), entre outros. 5.5.3 - Iniciativa: Implantar Sistema de Gestão de Segurança da Informação (normas ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002): Política de Segurança da Informação e de Ativos. OBJETIVO: APRIMORAR OS PROCESSOS INTERNOS DA PMDF.
>
> 10. OBJETIVO: GARANTIR AS INFORMAÇÕES NECESSÁRIAS À TOMADA DE DECISÃO. 10. Objetivo: Garantir as informações necessárias à tomada de decisão. Estratégias: 10.1. Desenvolver a atividade de Inteligência Policial. 10.1.12. Realizar estudos baseados em gestão da informação para integração dos dados do Sistema de Informações Policial Militar (SIPOM).
> 10.3. Dotar a Corporação de informações e sistemas de suporte à

> tomada de decisão e aos processos de gestão administrativa. Iniciativas Estratégicas: 10.3.6. Desenvolver e implantar projetos de Governança Corporativa, Gestão de Segurança da Informação (ISO 27.0000) e Gestão de Riscos (ISO 31.000).
>
> PERSPECTIVA DA CORPORAÇÃO 13. OBJETIVO: MAIOR CAPACIDADE DE PROTEÇÃO DOS ATIVOS. Contribui para o seguinte Objetivo do Plano Estratégico da PMDF:

Nesse sentido e demonstrando a importância estratégica do estabelecimento de práticas de segurança para a gestão da informação organizacional nas instituições, o Plano de Política de Governança de Tecnologia da Informação e Comunicação da Polícia Militar do Distrito Federal (PGTIC/PMDF), estabelecido pela portaria PMDF Nº 1096/201, considera em uma de suas diretrizes a segurança da informação de acordo o inciso II do artigo 7º, nos termos seguintes:

> Art. 7º O provimento de soluções de TIC observará as seguintes diretrizes:
> [...]
> II - consideração, quando da concepção de soluções de TIC a serem desenvolvidas ou adquiridas, de requisitos não funcionais relevantes, em especial dos requisitos de segurança da informação e dos requisitos relativos à disponibilidade, ao desempenho e à usabilidade da solução.
> [...]

Logo, é relevante pontuar que a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, não se aplica aos dados que constam nos sistemas de informação da corporação. Confira-se expressa disposição legal:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> [...]
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> [...]
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que

> serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

Em virtude da exceção legalmente determinada e considerando a vedação ao tratamento por pessoa jurídica de direito privado dos dados que envolvam segurança pública, defesa nacional, segurança do Estado e/ou atividades de investigação e repressão de infrações penais, como é o caso das informações constantes na base de dados da PMDF, especialmente por intermédio do sistema Gênesis, retoma-se a importância de que esse sistema seja analisado e aprimorado a fim de que haja segurança dos seus dados.

Desse modo, a criação e o desenvolvimento do produto garante a posterior identificação do Policial Militar responsável por eventual utilização indevida de dados existentes nos bancos de informação da Polícia Militar do Distrito Federal (não apenas do sistema Gênesis, foco inicial deste trabalho), notadamente porque, assim como a sua matrícula, o sinal identificador o acompanhará por toda a sua vida funcional, corroborando para que o Centro de Inteligência da PMDF possa melhor executar as suas atribuições e permitindo que os dados sejam melhor protegidos.

## 3.1 - ESTEGANOGRAFIA (referencial teórico)

O termo Esteganografia é derivado de duas palravas do grego, “*steganos*” – coberto e “*graphein*” – escrita, ou seja, “escrita oculta” (PETITCOLAS; ANDERSON; KHUN, 1999). Esteganografia, portanto, oriunda do grego significa "escrita escondida" é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma segurança até hoje usada nos mais diversos ramos.

Durante a idade média o primeiro uso registrado da palavra data do ano de 1499, no livro *Steganographia*, de Johannes Trithemius, um monge que escreveu uma série de livros chamados “Steganographia” em que descreveu várias técnicas diferentes. Mensagens também foram enviadas através de escravos de confiança.

Alguns reis raspavam as cabeças de escravos e tatuavam as mensagens nelas. Depois que o cabelo crescesse, o rei mandava o escravo pessoalmente com a mensagem (KAHN, 1996). Uma outra utilização era escrever a mensagem com tinta invisível sobre um papel, cortá-lo em alguns pedaços e depois rejuntá-los no destinatário (KAHN, 1996).

Nesse sentido é o ramo particular da criptologia que compreende fazer com que uma forma escrita seja dissimulada em outra a fim de ocultar o seu verdadeiro sentido. Ressalta se que há diferença em criptografia e esteganografia, ou seja, criptografia oculta o significado da mensagem e a esteganografia oculta a existência da mensagem.

> A segurança da informação é adotar controles físicos, tecnológicos e humanos personalizados, que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio (SÊMOLA, 2003, p. 35).

Essencialmente a escrita secreta se divide em duas partes: a criptografia e a esteganografia. A diferença entre elas está no fundamento, pois a criptografia deixa evidente que existe um dado e que o mesmo está cifrado. Por sua vez a esteganografia visa ocultar essa informação, e a mensagem é embutida em outro tipo de mídia, fazendo-se pensar que não há nada oculto (CARVALHO, 2008)

Assim temos com um exemplo dessa técnica a alteração de bits menos significativos de cada pixel de uma imagem colorida de forma que equivalente a uma mensagem, assim cada bit corresponderia a uma mensagem de maneira a não afetar significativamente o resultado visualizado na imagem. A técnica de funcionamento pode ser exemplificada como: uma imagem de 1024 por 768 pixels totaliza um arquivo de 786,432 pixels. Como cada pixel tem quatro bytes, pode-se esconder cerca de 390 kbytes de informação nessa imagem, isto é, mais ou menos sete linhas de um arquivo de bloco de notas (ROCHA, 2003).

Assim a esteganografia tem importância impar na segurança da tecnologia da informação, conforme o aumento da dependência das instituições perante as tecnologias, zelando do ativo mais valioso e vital para garantia do sucesso institucional, bem como a correta utilização de informações pessoais afetas ao trabalho de uma organização ou instituição. Aspectos que sempre serão fundamentais

em qualquer situação são: garantia da disponibilidade de recursos e informações, integridade da informação e confidencialidade da mesma (HOLANDA, 2006).

Em se tratando de informações afetas ao serviço policial militar e dos dados e informações geradas a cada atuação das diversas formas de policiamento, a confidencialidade da informação é um dos aspectos mais importantes, de modo que a informação seja somente disponibilizada a quem de direito, de forma a diminuir a possiblidade de acesso a informações desnecessárias (de cunho estratégico) e possíveis ataques ou uso indevido de informações ou mesmo seu vazamento. Com isso posto, a escrita secreta visa esconder um texto, a fim de que outra pessoa não saiba de sua existência (CARVALHO, 2008).

A técnica de esteganografia é um instrumento hábil que possibilita enfrentar esse desafio, fazendo com que, ao contrário da criptografia, usuários que realizem acesso as informações em um banco de dados não saiba que uma mensagem está sendo transmitida, desse modo a ferramenta em questão contribui para comunicações confidenciais por canais ou ambientes em tese não seguros, com fim da integridade da informação.

Para uma esteganografia efetiva, segundo Adhiya e Patil (2012), são necessárias algumas características fundamentais que devem ser verdadeiras em todo o processo de comunicação:

• Segredo: ninguém pode ser capaz de acessar o dado escondido sem ter a chave privada que é usada para extração.

• Imperceptibilidade: o meio com a informação não pode ser suspeito de manipulação.

• Alta capacidade: o meio deve ser grande o suficiente para o tamanho da informação.

• Resistência: a informação deve permanecer inalterada mesmo que se o meio em que trafega sofrer alguma manipulação.

• Extração precisa: quando o receptor extrair a informação, ela deve ser legível e confiável.

Divya e Thenmozhi (2016) propõem a existência de seis categorias para as técnicas esteganográficas nos meios digitais, são elas: Domínio espacial, espalhamento espectral, estatísticas, transformação de domínio (ou domínio da frequência), de distorção, mascaramento e filtragem. Cada uma dessas categorias

pode ter vários métodos de ocultamento da informação, com a aplicação entre eles variando de acordo com o meio que será usado na transmissão do dado.

### 3.1.1. Terminologia

Diante do interesse cada vez maior, por diferentes organizações e instituições, no campo da esteganografia, marcas d'água e seriação digitais. Dessa maneira pode ocorrer uma certa confusão na terminologia. A seguir, encontram-se alguns dos principais termos utilizados nestas áreas e ilustrados na Figura:

• dado embutido ou *embedded data* – é o dado que será enviado de maneira secreta, normalmente em uma mensagem, texto ou figura;

• mensagem de cobertura ou *cover-message* – é a mensagem que servirá para mascarar o dado embutido. Esta mensagem de cobertura pode ser de áudio (*cover-audio),* de texto (*cover-text*) ou uma imagem (*cover-image*);

• estego-objeto ou *stego-object* – após a inserção do dado embutido na mensagem de cobertura se obtém o estego-objeto;

• estego-chave ou *stego-key* – adicionalmente pode ser usada uma chave para se inserir os dados do dado embutido na mensagem de cobertura. A esta chave dá-se o nome de estego-chave;

• número de série digital ou marca *fingerprinting* – consiste em uma série de números embutidos no material que será protegido a fim de provar a autoria do documento.

Figura 1 - Escondendo uma imagem


Fonte: Petitcolas; Anderson; Kuhn (1999).

### 3.1.2 – Sistema de marcação marca d'água (*watermarking*)

O sistema de marcação tipo marca d'água é o método de camuflar informações em objetos que são robustos e resistentes a modificações. Assim é impossível remover uma marca d'água de um objeto sem alterar a qualidade visual da marca d'água.

Ressaltasse que a esteganografia se propõe a esconder uma informação em uma imagem de cobertura, de modo que se a imagem for modificada ou transformada a mensagem é perdida. Uma outra diferença elementar entre esteganografia e técnicas de marca d'água é que enquanto o dado camuflado na esteganografia nunca deverá ficar visível, na marca d'água pode ou não estar aparente no objeto marcado, dependendo da finalidade com que a aplicação da técnica queira atingir enquanto técnica de segurança da informação.

Destaca-se que as duas técnicas em questão pertencem a uma área de pesquisa no ramo da segurança da informação conhecida como ocultamento da informação (em inglês, *information hiding*).

Assim pode-se classificar os sistemas de marcação conforme com a sua robustez e a sua aparência. Segundo sua robustez, podem ser classificados como:

• robustos - são aqueles em que mesmo após a tentativa de remoção a marca permanece intacta;

• frágeis- são os sistemas em que qualquer tentativa de modificação na mídia acarreta a perda da marcação. É muito útil para verificação de cópias ilegais. Quando se copia um objeto original, a cópia é feita sem a marca.

E no que se refere a sua aparência, os sistemas de marcação podem ser classificados como:

• de marcação imperceptível - são os sistemas onde a marca encontra-se no objeto ou material, porém não é visível diretamente;

• de marcação visível - neste sistema a marca do autor deve ficar visível para comprovar a autoria visualmente. Um bom exemplo deste sistema são as marcas d´água em cédulas de dinheiro e em selos.

### 3.1.3 Estado da Arte e Requisitos

As imagens são as mídias de camuflagem mais populares para as técnicas e podem ser armazenadas em um formato BMP ou JPEG. Imagens de palheta de cores estão normalmente no formato GIF. O ocultamento de informações é realizado ou no domínio espacial ou no domínio de frequência. Em termos de esquemas de inserção, vários métodos (como substituição, adição e ajuste) podem ser usados. Uma abordagem de ajuste é a QIM (*Quantization Index Modulation*), que usa diferentes quantizadores para transportar diferentes bits dos dados secretos (SULLIVAN *et al*., 2004).

A utilização mais comum de inserção de mensagens em imagens inclui técnicas de inserção no bit menos significativo, técnicas de filtragem e mascaramento e algoritmos e transformações. Cada uma destas técnicas pode ser aplicada às imagens, com graus variados de sucesso. O método de inserção no bit menos significativo é provavelmente uma das melhores técnicas de esteganografia em imagem (PETITCOLAS; ANDERSON; KUHN, 1999; WAYNER, 2002).

Os três requisitos mais importantes que devem ser satisfeitos para qualquer sistema de camuflagem são:

• segurança - a fim de não levantar suspeita, enquanto tenta criar uma blindagem contra um algoritmo de descoberta, o conteúdo escondido deve ser invisível tanto perceptivelmente quanto por meios estatísticos (BUCCIGROSSI;

SIMONCELLI, 1999). Além disso, a complexidade computacional de qualquer ferramenta de esteganografia útil não pode ser infinitamente grande. Em termos de praticidade, um sistema pode ser considerado seguro, ou esteganograficamente forte (DUDA; HART; STORK, 2000), se não for possível descobrir a presença de stego-conteúdo usando qualquer meio acessível;

• carga útil - diferentemente de marca d'água, que precisa embutir somente uma quantia pequena de informações de direitos autorais, a esteganografia é direcionada à comunicação escondida e, portanto, normalmente exige capacidade de inclusão suficiente. Os requisitos para capacidade significativa de dados e segurança são frequentemente contraditórios. Dependendo dos argumentos de aplicação específica, um compromisso deve ser buscado;

• robustez - embora robustez contra ataques não seja uma prioridade importante, como em marcas d'água, ter a capacidade de resistir a compressão é certamente desejável, pois a maioria das imagens JPEG coloridas são comprimidas antes de serem colocadas on-line.

# 4 OBJETIVOS

## 4.1 *Objetivo geral*

Entregar, como produto, um sinal identificador gerado por intermédio de sistema de numeração binário, decimal e hexadecimal para cada Policial Militar.

## 4.2 *Objetivos específicos*

- Tornar cada tela de operação do sistema Gênesis única e identificável;
- Assegurar a identificação do Policial Militar responsável por eventual utilização indevida de dados existentes nos bancos de informação da Polícia Militar do Distrito Federal;
- Tornar os dados institucionais melhor protegidos.

## 5 BREVE DESCRIÇÃO DO PRODUTO

O produto consiste na criação e no desenvolvimento de um sinal identificador de autenticação individual para o sistema Gênesis que pretende evitar o vazamento de seus dados por *prints*, impressão e/ou foto da sua tela e, caso a má utilização dos dados aconteça, permitir a identificação e a imputação de responsabilidade do Policial Militar autor do fato, viabilizando a atuação do Centro de Inteligência e do Departamento de Controle e Correição da PMDF.

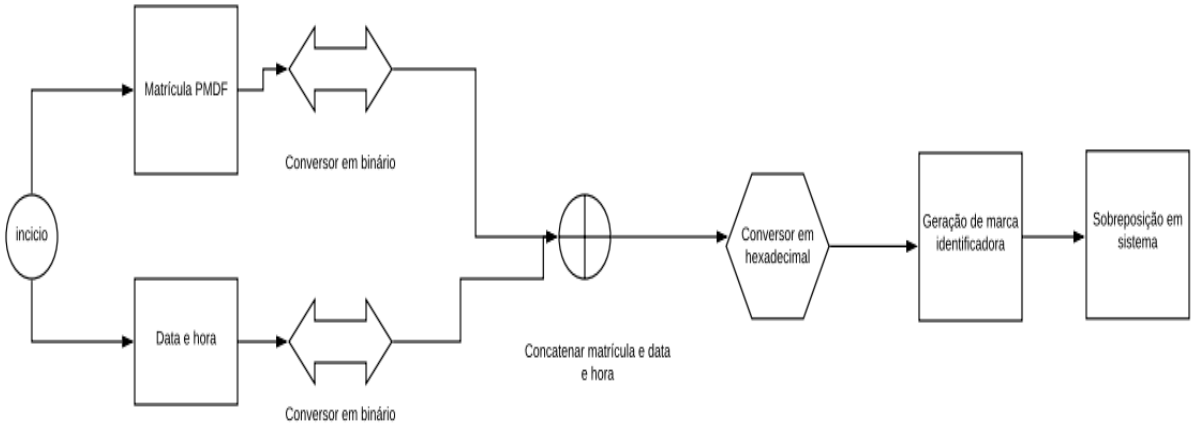
O sinal identificador é criado a partir da utilização de sistema de numeração binário, decimal e hexadecimal. Atualmente, o sistema mais comum de numeração é o decimal, sistema com somas em base “10” com 10 símbolos utilizados nas representações (0,1,2,3,4,5,6,7,8 e 9). Ele consiste na contagem dos números de “10” em “10”. Quando um número chega à contagem “9”, zera-se a contagem e adiciona-se o número “1” à frente do número. Por exemplo, o número cem em decimal é representado por 100 que é o mesmo que $1*100 + 0*10+0*1$ ou $1*10^2+0*10^1+0*10^0$.

Já o sistema binário é representado por somas em base “2”, apenas dois símbolos são utilizados (geralmente 0 e 1). O número 100 em binário seria representado em base “2” por 1100100 que é o mesmo que $1*2^6+1*2^5+0*2^4+0*2^3+1*2^2+0*2^1+0*2^0$ .

Por sua vez, o sistema hexadecimal é representado por somas em base “16”, 16 símbolos são utilizados (de 0 a 9 e A,B,C,D,E e F). Quando o número chega à contagem “9” continua com os símbolos A, B, C D e F e só então volta para “0”. O número 100 em base hexadecimal é representado por 64, que é o mesmo que $6*16^1+4*16^0$.

O fluxograma a seguir descreve o passo a passo da formação do sinal identificador único:

Figura 2 – Fluxograma de funcionamento do produto.




Elaboração: O autor.

Deve-se observar que, quando o usuário abre uma tela crítica do sistema (por exemplo a busca de pessoas ou escalas de serviços operacionais no Gênesis), sua matrícula é convertida em binário e concatenada à data e à hora de carregamento da tela. Os valores são, então, juntados em um único número binário e, após, convertidos para o sistema hexadecimal. Esse valor é adicionado a uma imagem e sobrepostos à tela do sistema visualizada pelo usuário, sem, contudo, interferir na visualização dos dados.

Para facilitar a visualização prática do produto, exemplifica-se: imagine que o usuário da matrícula 734756 acessou a página de pesquisa gênesis às 13:08 do dia 28/02/2021. O seu número de matrícula 734756 no sistema binário é representado por “10110011011000100100”. Já “280220211308” (data e horas concatenadas), é representado em binário por “10110011011000100100100000100111110011011010001100001101100”.

Concatenando os números em binário e convertendo para hexadecimal, gera-se o sinal “B3624827CDA30D”, que seria espelhado na marca d’água e sobreposto à tela do sistema, tal como apresentado na imagem a seguir.

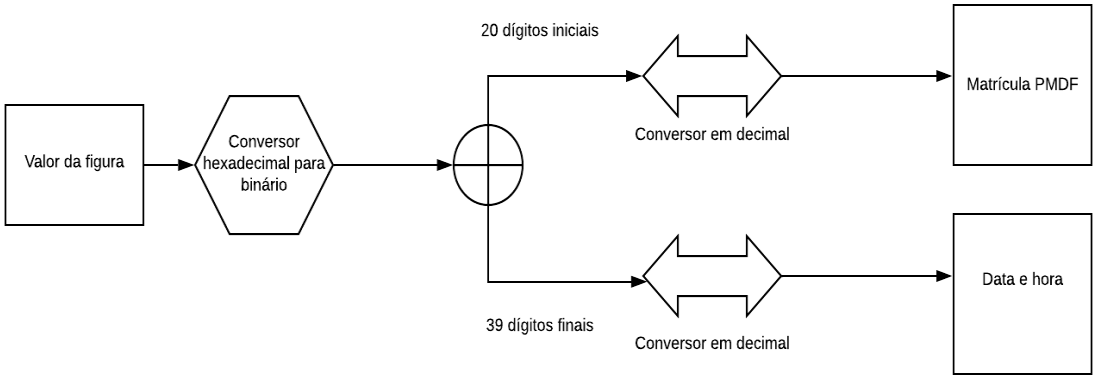
Figura 3 – Identificação tácita do login.


Elaboração: O autor.

Deve-se ressaltar que o sinal identificador único (B3624827CDA30D) é registrado em 3 pontos na figura sem obstruir as informações visualizadas na tela.

A identificação do Policial Militar usuário do sistema Gênesis e que tenha sido responsável pelo *print*, impressão e/ou foto da sua tela pode ser obtida a partir da operação reversa, representada no fluxograma a seguir:

Figura 4 – Fluxograma da transformação.

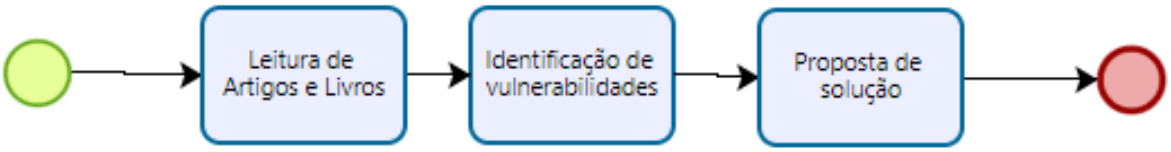



Elaboração: O autor.

O produto da pesquisa permite, portanto, a identificação do usuário que tenha sido responsável por *print*, impressão e/ou foto da tela do sistema Gênesis. O sinal identificador garante a segurança da informação e a utilização escorreita dos dados que constam dos sistemas da PMDF e pode contribuir com a sua melhor gestão e com a eventual responsabilização funcional no caso de má utilização daqueles.

## 6 METODOLOGIA

Figura 5 – Metodologia aplicada.




Elaboração: o autor.

A pesquisa aqui proposta visa gerar conhecimento a partir de uma aplicação prática da ciência e, deste modo, desenvolver um produto, sem ônus à instituição, a partir da solução de um problema específico. Isto e, trata-se de uma pesquisa aplicada, a qual segundo Prodanov e Freitas (2013, p. 51) “objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais.”.

Ademais, esta pesquisa se respaldará na abordagem qualitativa, uma vez que visa analisar, compreender e interpretar os diversos modelos de segurança da informação encontrados na literatura por meio de uma revisão bibliográfica. Vale ressaltar que tais modelos serão a base para o desenvolvimento do produto que melhor se aplique às necessidades e às vulnerabilidades institucionais encontradas.

Em relação à pesquisa qualitativa, Prodanov e Freitas (2013, p. 70) afirmam que

> Na abordagem qualitativa, a pesquisa tem o ambiente como fonte direta dos dados. O pesquisador mantém contato direto com o ambiente e o objeto de estudo em questão, necessitando de um trabalho mais intensivo de campo. Nesse caso, as questões são estudadas no ambiente em que elas se apresentam sem qualquer manipulação intencional do pesquisador. A utilização desse tipo de abordagem difere da abordagem quantitativa pelo fato de não utilizar dados estatísticos como o centro do processo de análise de um problema, não tendo, portanto, a prioridade de numerar ou medir unidades.

Em suma, a pesquisa qualitativa “[...] não está moldada na mensuração [dos dados] [...]” (FLICK, 2013, p. 23).

A análise, compreensão e interpretação dos dados relativos às supostas vulnerabilidades do sistema Gênesis foi realizada através pesquisa bibliográfica com pertinência temática em segurança da informação e no âmbito institucional junto ao centro de inteligência.

## 7 CONSIDERAÇÕES FINAIS

A revisão da literatura realizada até o presente momento identificou a relevância do estudo da segurança da informação, notadamente no setor público e especialmente nas áreas que tratam com dados cujo acesso é restrito. A partir de uma visão ampla da operação do sistema Gênesis, identificou-se suposta vulnerabilidade do instrumento na interação usuário/informação durante sua utilização.

Com base no contexto apresentado no decorrer deste projeto, pode-se constatar que é premente a criação e a operacionalização de uma ferramenta de segurança da informação a fim de que as restrições de divulgação e a responsabilização postos nas normas institucional tenham aplicabilidade e efetividade.

Logo, considerando a viabilidade do produto final proposto e tendo em vista as proposições dispostas no Planejamento Estratégico da Corporação, bem como àquelas alinhadas à Política de Governança de Tecnologia da Informação e Comunicação da Polícia Militar do Distrito Federal (PGTIC/PMDF), pretende-se garantir a identificação do(a) Policial Militar responsável por eventual utilização indevida de dados existentes nos bancos de informação da Polícia Militar do Distrito Federal (não apenas do sistema Gênesis, foco inicial deste trabalho). Tal intento se justifica notadamente porque, assim como a sua matrícula, o sinal identificador o(a) acompanhará por toda a sua vida funcional, corroborando para que o Centro de Inteligência da Polícia Militar do Distrito Federal possa melhor executar as suas atribuições e permitindo que os dados sejam melhor protegidos e com o Departamento de Controle e Correição da PMDF, possibilitando a formação de elementos de informações inerentes aos procedimentos administrativos de apurações criminais e disciplinares.

Sinais identificadores de autenticação revelam-se área de pesquisa extremamente ativa e necessária diante da constante ampliação das informações geradas com o serviço policial, o que reforça a importância do desenvolvimento desta pesquisa, especialmente no que diz respeito a solução de proteção de dados institucionais expostos na tela de operações do sistema Gênesis, sem ônus à Polícia Militar do Distrito Federal, pois sua implementação não gerará custos a instituição.

## REFERÊNCIAS

ADHIYA, K. P.; PATIL, Swati A.. Hiding Text in Audio Using LSB Based Steganography. *Information and Knowledge Management*, v. 2, n.3, p. 8-14, 2012. Disponível em: https://www.iiste.org/Journals/index.php/IKM/article/view/1782 Acesso: 01 jul. 2021.

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBR ISO/IEC27002. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2005.

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBR ISO/IEC27001. Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação – Requisitos*. Rio de Janeiro: ABNT, 2006.

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBRISO/IEC27005. Tecnologia da Informação - Técnicas de segurança - Gestão de riscos de segurança da informação*. Rio de Janeiro: ABNT, 2008.

AZAMBUJA, A. J.; NETO, J. S. Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal. *Revista do Serviço Público*, Brasília, v. 71, n. 3, p. 660-712, 2020. DOI: https://doi.org/10.21874/rsp.v71i3.3210 Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/3210. Acesso: 01 jul. 2021.

BARDIN, L. *Análise de conteúdo.* São Paulo: Edições 70, 2011.
BÖGER, D. S.; BODEMÜLLER JUNIOR, R. *Segurança da Informação.* 2007. Disponível em: http://www.das.ufsc.br/~dsboger/aula/07_1/ine5329-administracao_em_processamento_de_dados/transparencias_seguranca.pdf Acesso: 01 jul. 2021.

BRASÍLIA. Polícia Militar do Distrito Federal. Planejamento Estratégico da PMDF 2011/2021 Disponível em: http://www.pmdf.df.gov.br/imagens/Divulgacao/2016/planejamentoestrategico/3ed.pdf Acesso: 01 jul. 2021.

BRITTO, T. D. e. *Levantamento e diagnóstico de maturidade da governança da segurança da informação na administração direta federal brasileira*. 2011. 146 f. Dissertação (Mestrado em Informática) - Universidade Católica de Brasília, Brasília, 2011. Disponível em: https://bdtd.ucb.br:8443/jspui/handle/123456789/1331 Acesso: 01 jul. 2021.

BUCCIGROSSI, R. W.; SIMONCELLI, E. P. Image compression via joint statistical characterization in the wavelet domain. *IEEE Transactions on Image Processing*, v. 8, n. 12, p. 1688–1701, 1999. Disponível em: https://ieeexplore.ieee.org/abstract/document/806616 Acesso: 01 jul. 2021.

CARVALHO, D. F. Esteganografia digital para transmissão oculta de mensagens. Disponível em: http://stoa.usp.br/diegofdc/files/-1/4188/EsteganografiaDigitalPalestra.pdf Acesso: 01 jul. 2021.

COLWILL, C. *Human factors in information security*: The insider threat & Who can you trust these days?. *Information Security Technical Report* 14, p. 186-196, 2009. Disponível em: https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/Previous%20Articles/Ch11InternalThreatsUsers.pdf Acesso: 01 jul. 2021

CUNHA, M.; CAVALCANTI, C. Dicionário de Biblioteconomia e Arquivologia. Brasília: Briquet de Lemos. 2008.

DIVYA, A.; THENMOZHI, S. Steganography: Various Techniques in Spatial and Transform Domain. *International Journal of Advanced Scientific Research and Management*, v. 1, p 81-89, 2016. Disponível em: http://ijasrm.com/wp-content/uploads/2016/03/IJASRM_V1S3_029_81_89.pdf Acesso: 01 jul. 2021.

DUDA, R. O.; STORK, David G.; HART, Peter. E. *Pattern* Classification. 2 ed. EUA: Wiley-Interscience, 2000.

FLICK, U. *Introdução à metodologia de pesquisa*: um guia para iniciantes. Traduzido por: Magda Lopes. Porto Alegre: Penso, 2013, 256p.

HOLANDA, R. de. O estado da arte em sistemas de gestão da segurança da informação: norma ISO/IEC 27001: 2005. São Paulo: Módulo Security Magazine, 2006.

IETF. Request for Comments (RFC). 2017. Disponível em: www.ietf.org/rfc.html. Acesso: 01 jul. 2021.

ISACA. Information Systems Audit and Control Association. *Cobit 5.0, modelo corporativo para governança e gestão de TI da organização*. 2012.

KRAEMERA, S.; CARAYON, P.; CLEM, J. Human and organizational factors in computer and information security: Pathways to Vulnerabilities. *Computer & Security*, v. 28, p. 509-520, 2009. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404809000467 Acesso: 01 jul. 2021.

MANOEL, S. da S.. *Governança de segurança da informação*: como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014.

MCDANIEL, G.. IBM Dicitionary of Computing. New York, NY: McGraw-Hill, 1994.

NOBRE, A. C. S; RAMOS, A. S. M; NASCIMENTO, T. C. *Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação:* um estudo com gestores públicos estaduais no Brasil. Rio de Janeiro: XXXIV Anpad, 2010.

PELTIER, T. R. *Information security risk analysis*. Boca Raton: Auerbach Publications, 2001.

PETITCOLAS, F. A. P.; ANDERSON, R. J.; KUHN, M. G. Information hiding — A survey. *Proceedings of the IEEE*, v. 87, n. 7, p. 1062–1078, 1999. Disponível em: https://ieeexplore.ieee.org/document/771065 Acesso: 01 jul. 2021.

Polícia Militar do Distrito Federal. *PORTARIA PMDF Nº 1019, DE 30 DE SETEMBRO DE 2016*. Institui no âmbito da Corporação o Sistema de Gerenciamento Operacional e Cadastro de Atendimentos e Ocorrências da PMDF, denominado Gênesis, regulamenta seu preenchimento e dá outras providências. Disponível em https://intranet.pmdf.df.gov.br/controleLegislacao2/PDF/2152.pdf. Acesso: 01 jul. 2021.

Polícia Militar do Distrito Federal. PORTARIA PMDF Nº 1096, DE 11 DE JUNHO DE 2019. Estabelece a Política de Governança de Tecnologia da Informação e Comunicação da PMDF (PGTIC/PMDF). Disponível em: https://intranet.pmdf.df.gov.br/controleLegislacao2/PDF/2299.pdf. Acesso: 01 jul. 2021.

PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico:* métodos e técnicas da pesquisa e do trabalho acadêmico. 2 ed. Novo Hamburgo: Feevale, 2013.

RAHMAN, H. A.; MARTI, J. R.; SRIVASTAVA, K. D. A. Hybrid systems model to simulate cyber interdependencies between critical infrastructures. *International Journal of Critical Infrastructures*, Inderscience Enterprises Ltd, v. 7, n. 4, p. 265-288, 2011. Disponível em: https://ideas.repec.org/a/ids/ijcist/v7y2011i4p265-288.html Acesso: 01 jul. 2021.

RAMOS, A. *Security Officer:* guia oficial para formação de gestores em segurança da informação*.* Porto Alegre: Zouk, 2006.

ROCHA, A. de R. *Camaleão: um software digital utilizando esteganografia*. 2003. Monografia (Bacharelado em Ciência da Computação) – Departamento de Ciência da Computação, Universidade Federal de Lavras, Lavras, 2003.Disponível em: http://repositorio.ufla.br/handle/1/9340 Acesso: 01 jul. 2021.

SANTOS, L. A. F. d. *Segurança da informação.* 2011. Disponível em: www.slideshare.net/ luiz_arthur/seguranca-da-informao-introduo. Acesso: 01 jul. 2021.

SÊMOLA, M. *Gestão da segurança da informação*: visão executiva. Rio de Janeiro: Elsevier, 2003.

SIEWERT, V. C. *A Constante Evolução da Segurança da Informação.* 2008. Disponível em: http://www.artigocientifico.com.br/uploads/artc_1202929819_49.pdf Acesso: 01 jul. 2021.

SOARES, E. Polícia Militar do Distrito Federal. *Polícia Militar completa 210 anos com os olhos voltados para o futuro*. 13 de maio de 2019. Disponível em: http://www.pmdf.df.gov.br/index.php/institucionais/23857-policia-militar-completa210-anos-com-os-olhos-voltados-para-o-futuro. Acesso: 01 jul. 2021.

SULLIVAN, K. *et al*. Steganalysis of quantization index modulation data hiding. *IEEE International Conference on Image Processing*, v. 2, p. 1165 – 1168, 2004. Disponível em: https://ieeexplore.ieee.org/abstract/document/1419511 Acesso: 01 jul. 2021.

SUMMERS, R. C. *Secure computing: threats and safeguards*. New York: McGraw-Hill, 1997.

SVEEN, F. O.; TORRES, J. M.; SARRIEGI, J. M. Blind Information Security Strategy. *International Journal of Critical infrastructure Protection*, v.2, p.95-109, 2009.

WAYNER, P. *Disappearing Cryptography*: Information Hiding: Steganography and Watermarking. 2 ed. San Francisco, EUA: Morgan Kaufmann Publishers, 2002.

YAHYA*,* A. *Steganography Techniques for Digital Images.* EUA: Springer International Publishing, 2019.