# A CONTRAINTELIGÊNCIA NA GESTÃO DE PESSOAL NA ADMINISTRAÇÃO PÚBLICA

**Renato Augusto Lyrio Ramos**[1]
**Paula Cristina Pedroso Moi**[2]

**Resumo**

Este trabalho tem como objetivo identificar e descrever características e procedimentos de contrainteligência na segurança orgânica no que tange à gestão de pessoal. Além disso apresenta medidas desejáveis de contrainteligência na gestão de pessoal na Administração Pública. Foi realizada uma revisão de literatura com pesquisa documental em acervos específicos de Contrainteligência e gestão de pessoal. Para orientar o desenvolvimento, buscou-se abordar conceitos de Contrainteligência, segurança orgânica, pormenorizando os procedimentos a serem adotados na segurança dos recursos humanos e da informação no pessoal, tendo como linha de balizamento a Administração Pública. Por fim, conclui-se que o desenvolvimento de uma mentalidade de proteção dos ativos ou mentalidade de contrainteligência é um dos fatores mais importes dentro da segurança orgânica dos recursos humanos e da informação no pessoal. Além disso, sugere-se procedimentos para diagnosticar e executar ações que sirvam para gerir os riscos ligados diretamente ao ser humano no contexto da Contrainteligência e Administração Pública.

**Palavras chaves:** Contrainteligência, Gestão de Pessoal, Administração Pública, Segurança Orgânica, Mentalidade de Contrainteligência.

# CONTRAINTELIGENCE IN STAFF MANAGEMENT IN PUBLIC ADMINISTRATION

**Abstract**

This work aims to identify and describe counterintelligence characteristics and procedures in organic security with regard to personnel management. In addition, it presents desirable counterintelligence measures in personnel management in Public Administration. A literature review was carried out with documentary research in specific collections of Counterintelligence and personnel management. To guide development, we sought to address concepts of Counterintelligence, organic security, detailing the procedures to be adopted in the security of human resources and information in personnel, with the Public Administration as a guideline. Finally, it is concluded that the development of an asset protection mentality or counterintelligence mentality is one of the most important factors within the organic security of human resources and personnel information. In addition, procedures are suggested to diagnose and carry out actions that serve to manage risks directly linked to human beings in the context of Counterintelligence and Public Administration.

[1] Pós-Graduando de Gestão em Administração Pública, graduado em Ciências Bélicas e Militares pela Academia Militar das Agulhas Negras. E-mail: ofaugustoramos@yahoo.com.br
[2] Mestre em Economia pela Universidade Federal de Mato Grosso. E-mail: paulacpmoi@gmail.com

**Keywords:** Counterintelligence, Personnel Management, Public Administration, Organic Security, Counterintelligence mentality.

## 1 INTRODUÇÃO

O elemento humano é o elo mais fraco na segurança de uma Instituição. Porém, sem dúvidas, é o elo mais importante. “Desenvolver a mentalidade de Contrainteligência é um objetivo que deve ser buscado de forma permanente. A conscientização do público interno contribui para reduzir as deficiências e dificultar a atuação das ameaças.” (BRASIL, 2019 c, p. 1-5)

Dentro do ambiente organizacional na Administração Pública, a dimensão informacional tem demonstrado a relevância do elemento humano, quando a maioria de erros de processos, fraudes, ilicitudes administrativas provêm de pessoas que se aproveitam das vulnerabilidades encontradas em seus ambientes de trabalho.

Oliveira e Silva (2016), explicam que a chamada Administração de Pessoal Civil, hoje a Administração Pública Federal, passou ser alvo de estudos e mudanças a partir da década de 1930, impulsionada pelas mudanças político-sócio-econômicas da Revolução de 1930, liderada Getúlio Vargas.

Até aquele momento, as normas reguladoras sobre administração pública eram inexistentes. As funções dentro da Administração e salários pagos aos ocupantes dos cargos eram arbitradas pelos órgãos diversos do governo, sem ou com pouco controle. A política influenciava diretamente na maioria dos cargos disponíveis, não somente nos chamados comissionados ou de confiança (Oliveira e Silva, 2016).

No âmbito militar, a administração de pessoal já era regida por regulamentos, estudos e distribuição ordenada de claros administrativos das três Forças: Exército, Marinha e Aeronáutica.

Nesse contexto, Oliveira e Silva (2016), classificam algumas fases ou subsistemas de Gestão de Pessoas, associando-os às funções que serão desempenhadas. O sistema de Gestão de Pessoal é amplo e envolve todos os subsistemas (fases) apresentados no quadro abaixo:

Quadro 1 – Classificação dos subsistemas de gestão de Pessoas

| Função | Objetivo | Subsistema |
|---|---|---|
| Provisão | Indicar quem irá trabalhar na organização | Recrutamento e Seleção |
| Aplicação | Definir o que as pessoas devem fazer e verificar como fizeram | Cargos e Carreiras<br>Avaliação de Desempenho |
| Manutenção | Como manter as pessoas | Remuneração (salários e benefícios)<br>Qualidade de Vida no Trabalho |
| Desenvolvimento | Como preparar as pessoas | Treinamento<br>Desenvolvimento |
| Controle | Como saber quem são e o que fazem | Sistemas de informação<br>Registro e Controle |

Fonte: Oliveira e Silva (2016).

De acordo com o Manual de Campanha de Contrainteligência (BRASIL, 2019 c), a gestão de Recursos Humanos e sua respectiva segurança, consiste no grupo de medidas destinadas a preservar a integridade física e moral dos recursos humanos do Exército Brasileiro.

Os recursos humanos são os bens mais importantes do Exército e precisam ser protegidos e preservados (BRASIL, 2019 c). É possível estender essa afirmação para todo servidor da administração Pública.

A concentração de informações em pessoas e sistemas tem se tornado um problema para segurança. A Segurança da Informação cresce de importância pois são necessárias medidas de proteção a fim de se mitigar danos com eventuais perdas dessas informações (BRASIL, 2019 c).

A Segurança da Informação na administração Pública, particularmente as informações que cada pessoa carrega ou tem acesso merece especial atenção. Os órgãos ou instituições públicas possuem colaboradores, informações de licitações, processos administrativos diversos, informações pessoais e de pagamento, dentre outras, e devem ser protegidas, pois a perda, vazamento ou exposição desses dados pode trazer desgaste financeiro, administrativo ou para a imagem da instituição afetada.

Neste sentido, o presente trabalho possui a intenção de identificar e descrever características e procedimentos de contrainteligência na segurança orgânica no que tange à gestão de pessoal, além de apresentar medidas desejáveis de contrainteligência na gestão de pessoal na Administração Pública. A análise apresentada contemplará definições de segurança orgânica, visando o entendimento do assunto abordado.

Desta forma, tem por finalidade contribuir na atualização doutrinária referente ao Segmento da Segurança Orgânica do ramo de Contrainteligência no Grupo de Medidas de Segurança de Recursos Humanos e Segurança da Informação no Pessoal. Além disso, contribuir, também, para o desenvolvimento de uma mentalidade de contrainteligência nos órgãos e instituições da Administração Pública.

A pesquisa será baseada em uma pesquisa documental que selecionou instruções normativas e portarias sobre o assunto abordado, como a Instrução Normativa STJ/GP N. 12 de 6 de maio de 2019; Portaria CNEN-PR n. 012, de 23 de março de 2018; Portaria PGR/MPF n. 417 de 5 de julho de 2013; e Portaria n. 076 COTER, de 09 de julho de 2019. Este tipo de pesquisa poderá ser classificada, quanto à sua natureza como pesquisa aplicada e quanto ao tipo de pesquisa será classificada como bibliográfica.

Para tanto, o presente estudo foi pensado e dividido em capítulos onde serão conceituados e desenvolvidos os seguintes assuntos, respectivamente: Segurança Orgânica e seus grupos de medidas, a Segurança dos Recursos Humanos e medidas protetivas, Segurança da Informação, subgrupo da Segurança da Informação no Pessoal e medidas protetivas.

## 2 A CONTRAINTELIGÊNCIA NA GESTÃO DE PESSOAL NA ADMINISTRAÇÃO PÚBLICA

Segundo a Polícia Civil do Estado do Paraná (PARANÁ, 2020), a Contrainteligência tem a finalidade de produzir conhecimentos para neutralizar as ações adversas, e proteger a atividade e a instituição a que pertence. Na Contrainteligência estão enquadradas as atividades de Segurança Orgânica (Seg Org) e Segurança Ativa (Seg Atv).

O Manual de Campanha EB70-MC-10.220 tem um conceito mais completo de Contrainteligência. Ela é definida como “o ramo da Atividade de Inteligência, com objetivo de prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar ações de qualquer

natureza que constituem ameaças a salvaguarda de dados, conhecimentos, áreas, instalações, pessoas e meios que a Instituição tenha interesse de preservar". (BRASIL, 2019 c, p. 1)

A continuidade dos serviços prestados pela Administração Pública pode ser afetada por alguns fatores, tais como: ameaças provenientes da ação humana ou de catástrofes da natureza e a ocorrência de falhas de qualquer tipo. As vulnerabilidades relacionadas à estrutura física, sistemas de proteção pessoal (física ou técnica), processos, operações ou de outras áreas que possam ser alvos de incidentes, se exploradas, também podem vir a prejudicar ou interromper a prestação dos serviços (BRASIL, 2019 c).

Nesse escopo, a adoção de medidas de Contrainteligência se mostra bastante adequada na proteção da Administração Pública, particularmente seu pessoal. Elas se destinam a salvaguardar ativos, conforme definição de BRASIL (2019 c), em que cada um dos integrantes da Instituição (aqui entende-se qualquer órgão ou instituição pública) tem responsabilidades para com as atividades e tarefas de proteção da Administração como um todo. Envolve comportamentos, atitudes preventivas, proatividade e adoção consciente de medidas efetivas.

### 2.1. Segurança Orgânica

A Polícia Civil do Estado do Paraná (PARANÁ, 2020) define a Seg Org como o conjunto de normas, medidas e procedimentos com a finalidade defensiva, a fim de garantir que a instituição continue funcionando, de modo a prevenir e obstruir as ações adversas de qualquer natureza. Em linhas gerais, é um conjunto de medidas integradas e planejadas, destinadas a proteger os ativos institucionais (tangíveis e intangíveis), em especial, o pessoal, a documentação, as instalações, o material, as operações da instituição, as comunicações e a informática.

BRASIL (2019 c) apresenta a necessidade da criação, o desenvolvimento e a manutenção de uma mentalidade de Contrainteligência em toda a estrutura hierárquica da administração, visando a obtenção de um grau de proteção ideal.

### 2.2. Grupos de medidas da Segurança Orgânica

O BRASIL (2020 a), em sua Instrução Normativa STJ/GP n. 12 de 6 de maio de 2019, divide a Seg Org, didaticamente, nos seguintes grupos de medidas:

a. Segurança de pessoas;

b. Segurança da Informação;

c. Segurança do Material; e

d. Segurança das Áreas e instalações.

O Conselho Nacional do Ministério Público (CNMP, 2020), em sua Política de Segurança Institucional, também divide a Seg Org nesses grupos de medidas.

O CNMP explica que a segurança de pessoas reúne o conjunto de medidas voltadas a proteger a integridade física e moral de membros, ativos e inativos, de servidores e de seus respectivos familiares em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais. Problemas relacionados à segurança do indivíduo, sua saúde, acidentes sofridos, condições psicológicas devem receber especial atenção da diretoria.

CNMP continua sua definição ao dizer que ações relacionadas com a segurança de pessoas abrangem operações de segurança, atividades planejadas e coordenadas, com emprego de pessoal, material e equipamento especializado. Essas ações podem ser realizadas com pessoal orgânico da instituição, desde que instruído ou por órgãos externos.

Ainda, a segurança de material é o conjunto de medidas voltadas a proteger o patrimônio físico e bens, pertencente ou sob o uso da Instituição.

Dantas Filho (2004) defende que toda empresa, organização ou instituição deve planejar, confeccionar e possuir um plano de segurança e programa de instrução sobre segurança. Além disso, para o autor fica claro a preocupação que os chefes devem ter sobre o aspecto humano, o material e das áreas e instalações da instituição.

Dantas Filho (2004) define que a segurança de áreas e instalações compreende o conjunto de medidas voltadas a proteger o espaço físico sob responsabilidade da instituição ou onde se realizam atividades de interesse dela, bem como seus perímetros, com a finalidade de salvaguardá-las. Segundo Dantas Filho, essa segurança deve tornar o acesso à instituição completamente seguro, de modo a desestimular o indivíduo mal-intencionado de sua ação criminosa.

O CNMP (2020) preconiza que as áreas e instalações que abriguem informações sensíveis ou sigilosas e as consideradas vitais para o pleno funcionamento da Instituição serão objeto de especial proteção.

Ainda com o conceito do CNMP (2020), a Segurança da Informação é um grupo de medidas que visam proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados acarretará prejuízo de qualquer natureza para a instituição responsável pelos dados ou informações ou proporcionar vantagem a chamados atores antagônicos. No caso da administração pública, atores antagônicos podem ser a funcionários terceirizados ou orgânicos insatisfeitos, prestadores de serviço temporário, dentre outros.

### 2.3. Segurança dos Recursos Humanos

Até o século passado, as organizações industriais e prestadoras de serviços, em geral, visavam principalmente a eficiência e a produtividade dos processos adotados, deixando o ser humano em segundo plano, uma realidade que tem se modificado a cada dia. Para Chiavenato (2014) existe uma grande diferença entre gerenciar pessoas e gerenciar com pessoas:

> "No primeiro caso, os processos de desenvolver pessoas são fundamentais para o sucesso organizacional e se tornam estratégicos para a organização. No segundo caso, os processos de agregar pessoas ocupam o pódio e passam a ser estratégicos para a organização." (CHIAVENATO, 2014, p.73).

Com o passar dos anos, o Recurso Humano se tornou o principal ativo de qualquer instituição. A maioria dos problemas de segurança enfrentados pelas organizações estão relacionados com algum tipo de falha dos seus recursos humanos. Contudo, quando se fala em Administração Pública, cresce de importância os cuidados a serem tomados para bem selecionar o pessoal e evitar que sejam utilizados como meio para a consecução de fins favoráveis às ações adversas. (BRASIL, 2019 c)

A Comissão Nacional de Energia Nuclear (2020) definiu, em Portaria, que a segurança de recursos humanos é o conjunto de medidas voltadas a proteger a integridade física de servidores e colaboradores. No próprio desempenho das funções institucionais, cada servidor está exposto a riscos, concretos ou potenciais.

BRASIL (2019 c) descreve que, para assegurar um grau de segurança ideal no que concerne a proteção do pessoal, são adotadas medidas para fazer face as ameaças a esse ativo, considerando-se:

a) a possibilidade de que um integrante do público interno seja vítima de ilícito ou irregularidade;

b) a utilização de integrante da instituição para atos de espionagem, tanto como agentes infiltrados quanto pela exploração de suas eventuais deficiências;

c) atos de terrorismo, que podem afetar a integridade física do pessoal;

d) utilização de ação psicológica direcionada a interferir no moral e na disciplina do pessoal;

e) a desinformação, pela possibilidade de influenciar o processo de tomada de decisão;

f) qualquer ação de natureza hostil, que atente contra a integridade física de integrantes do público interno;

g) acidentes, de naturezas diversas, que podem causar danos ao pessoal, incluindo-se os fenômenos naturais; e

### 2.3.1. Medidas protetivas

As medidas de Segurança dos Recursos Humanos são estabelecidas, após uma análise minuciosa das ameaças.

Segundo BRASIL (2019 c), ameaças são o resultado da equação do ator, capacidade de agir e motivação. O ator pode ser qualquer indivíduo, interno à organização ou instituição. São pessoas que trabalham ou já trabalharam no ambiente, além daquelas que podem ter acesso, como distribuidores, colaboradores, parentes de servidores ou, até mesmo, algum fenômeno natural. A capacidade de agir é o potencial de um ator realizar uma ação. Devem ser considerados seus recursos e conhecimentos, além de sua liberdade para realizar uma tarefa.

BRASIL (2019 c) complementa que a motivação é um estado interno que resulta de uma necessidade do ator, dirigindo o comportamento humano para a satisfação dessa necessidade. O ator pode se motivar por ressentimento, vaidade, vingança, estresse, insatisfação, problemas financeiros, dentre outros motivos.

Oliveira e Silva (2016) destaca que, de um modo geral, a área de Gestão de Pessoas é tida como uma unidade estratégica nas organizações públicas ou privadas. Há diferentes fatores que são importantes, mas um em particular pode ser destacado, o reconhecimento de que as pessoas são essenciais para o alcance de resultados organizacionais. As autoras completam com a ideia de que a Gestão de Pessoas é responsável pelo desenvolvimento e implementação de políticas e práticas voltadas para os colaboradores na organização,

inclusive a sua proteção. Nesta perspectiva, é importante destacar que o treinamento e conscientização de pessoal para cumprimento de suas funções e desenvolvimento de ações proativas são importantes para a segurança.

BRASIL (2019 c) aponta diretamente que, dentre as medidas de segurança, destaca-se o exercício da ação de comando, ou seja, atitudes e medidas das chefias em todos os níveis. Deve-se reforçar, nos integrantes das organizações, os valores éticos e morais que norteiam a Instituição.

### 2.4. Segurança da Informação

Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. (BISHOP, 2003). Traduz-se em tudo aquilo que permite a aquisição de conhecimento. Segundo BRASIL (2019 c):

> A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou difundida verbalmente. Seja qual for a sua forma, ou o meio pelo qual é compartilhada ou armazenada, é necessário que a informação seja protegida. (BRASIL, 2019 c, p. 3-11)

A segurança da informação (Seg Info) está diretamente relacionada com a proteção desses ativos, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. "É obtida a partir da implementação de uma série de controles estabelecidos, para garantir que os objetivos de segurança específicos sejam atendidos" (BRASIL, 2019 c, p. 3-11).

GHODDOSI (2016) afirma que a informação passou a ser considerada importante para as empresas em função de sua dependência em tecnologia de informação. No cenário atual, não há organização que direta ou indiretamente seja independente da tecnologia e da informação. O autor acrescenta, ainda, que estas informações podem ser consideradas como um dos ativos mais valiosos das organizações ou empresas, pois possuem um valor muitas vezes incalculável não somente para a organização que a gerou, como para instituições ou atores hostis.

BRASIL (2019 c) elenca, dentre outro princípios da segurança da informação os seguintes aspectos: confidencialidade, integridade e disponibilidade, toda ação que poderá comprometer um desses princípios pode ser tratada como atentado a sua segurança.

Confidencialidade se define como a garantia de que a informação é acessível somente por pessoas autorizadas. Já a integridade é a preservação da exatidão da informação e dos métodos de processamento e disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário BRASIL (2019 c).

### 2.5. Subgrupo da Segurança da Informação no Pessoal

A Comissão Nacional de Energia Nuclear (CNEN) (BRASIL, 2020 c), em sua Portaria Nr 12, de 23 de março de 2018, define a segurança da informação nos recursos humanos como o subgrupo que compreende um conjunto de medidas voltadas a assegurar comportamentos adequados dos servidores da instituição ou terceiros que garantam a salvaguarda de informações sensíveis ou sigilosas.

O BRASIL (2020 a) divide a Seg Info Pes em:

I – Segurança no processo seletivo, no desempenho da função e no desligamento da função ou da instituição;

II – detecção, identificação, prevenção e gerenciamento de infiltrações, recrutamentos e outras ações adversas de obtenção indevida de informações;

III – identificação precisa, atualizada e detalhada das pessoas em atuação na instituição;

IV – verificação e monitoramento de ações de prestadores de serviços.

O BRASIL (2020 b) e o BRASIL (2020 a) destacam a necessidade da assinatura do Termo de Compromisso e Manutenção de Sigilo (TCMS) por parte de todos os funcionários que têm ou terão acesso a informações consideradas sigilosas ou sensíveis.

Ambas a instituições recomendam, ainda, que toda organização com a qual a instituição compartilhe informações sensíveis ou sigilosas possua normatização para compartimentação e preservação do sigilo de informações compartilhadas.

#### 2.5.1. Medidas protetivas

As organizações devem investir recursos e tempo para adotar processos eficientes de seleção, e que sejam compatíveis com suas regulamentações internas e a criticidade de suas informações. A rigidez desses controles deve ser diretamente proporcional à relevância do ativo ao qual o funcionário terá acesso, de acordo com o que se segue:

> "O processo de recrutamento e seleção para ocupar um determinado cargo/função de uma organização, principalmente em uma área estratégica, sensível ou vital, deve ser planejado de forma cautelosa. Esse processo visa, acima de tudo, selecionar a pessoa certa, com as habilidades, competências (influência, desenvolvimentos de pessoas, habilidades para gerenciar mudanças, liderança de pessoas) e as principais características comportamentais (capacidade de trabalhar sob pressão, resiliência, perseverança, autoconfiança, capacidade de tomada de decisões em um curto espaço de tempo), requeridas para desempenhar tal atividade." (PADILHA, 2010, p.1)

BRASIL (2019 c) aponta que medidas como a pesquisa social é outra importante etapa da seleção. A investigação da vida pregressa do candidato permite: ratificar as informações contidas no seu currículo e confirmar as qualificações acadêmicas e profissionais.

A mesma fonte destaca que é importante que todos os funcionários compreendam plenamente suas responsabilidades e estejam de acordo com seus papéis. As responsabilidades não devem ser atribuídas a indivíduos, mas sim a cargos ou posições dentro da estrutura da organização.

BRASIL (2019 c) também aponta a importância de garantir que a "passagem de função" aconteça de forma clara, objetiva e sem "traumas" para o ocupante do cargo que receberá todo o conhecimento produzido armazenado de forma segura e correta (backup), a fim de evitar que não haja represálias ou retaliações por parte de quem esteja saindo da função.

O conhecimento das informações sensíveis é essencial para a criação de mecanismos que impeçam seu vazamento. Durante todo o tempo em que o funcionário estiver contratado deve ser assegurado que os mesmos estejam conscientes de suas responsabilidades de segurança e conscientes das ameaças existentes (BRASIL, 2019 c).

Os programas de segurança implementados só terão o sucesso desejado se houver a aceitação e o envolvimento de todos. "É preciso desenvolver uma campanha de conscientização que promova mudanças de comportamento e, também, de cultura, de modo a estabelecer a necessidade de segurança." (MACEDO, 2013)

O desligamento de qualquer funcionário também requer a adoção de alguns procedimentos. É necessário atentar para a devolução de equipamentos e cartões de acesso disponibilizados para o desenvolvimento das atividades, de forma a retirar o acesso aos ativos (BRASIL, 2019 c).

A CNEN (2020) também elenca uma série de medidas protetivas em cada subgrupo de medidas, sendo as de segurança da informação de pessoas as seguintes:

Na Segurança no Desligamento, as instituições devem seguir as seguintes orientações:

I - O afastamento de função que trata de assuntos sigilosos deve ser realizado gradativa e paulatinamente, de forma a ocorrer uma desmobilização controlada, caso seja necessário;

II - Os membros e servidores que tenham acesso, por força de sua função, a sistemas ou serviços que tratem de assuntos sigilosos ou sensíveis, devem ser excluídos do acesso por ocasião de seu desligamento da função;

III - Para efeito do item anterior, as chefias imediatas e os setores de recursos humanos devem informar aos gerentes de cada sistema ou serviço sobre o afastamento das funções por membros e servidores. Os gerentes de cada sistema ou serviço que trate de assuntos sigilosos ou sensíveis devem avaliar periodicamente os seus respectivos sistemas ou serviços para identificar acessos indevidos. Nesse aspecto, é necessário um sistema informacional em condições de auditoria.

A Necessidade da assinatura do TCMS que é um documento que representa o compromisso formal do signatário em manter confidencialidade a respeito de dados e informações a que tenha acesso por força de suas funções. As instituições devem seguir as seguintes orientações:

I - Cada unidade deverá estabelecer um modelo próprio de Termo de Compromisso de Confidencialidade, de acordo com a especificidade de cada local;

II - O Termo de Compromisso de Confidencialidade deve ser arquivado em local seguro e estar disponível para consulta e auditoria.

## 3 CONSIDERAÇÕES FINAIS

A Administração Pública é regida por cinco princípios básicos: legalidade, impessoalidade, moralidade, publicidade e eficiência. Nota-se, em todos os princípios, o elemento humano como executor e garantidor deles. Cresce de importância a implementação de procedimentos de contrainteligência na gestão de pessoal.

Esta pesquisa apresentou os procedimentos de contrainteligência na gestão de pessoal a fim de garantir a segurança física do servidor ou funcionário e a informação que o próprio recurso humano carrega em sua bagagem cognitiva.

A principal contribuição deste trabalho é a de despertar a importância para o desenvolvimento de uma mentalidade de proteção dos ativos, já anunciada como mentalidade de contrainteligência. Essa mentalidade surge com palestras de conscientização, campanhas com panfletos ou avisos nos corredores do ambiente de trabalho, além do acompanhamento do pessoal de recursos humanos da Instituição. Além disso, deve haver medidas protetivas antes da ocupação do cargo, durante o desempenho da função e no desligamento do servidor.

Dentro desta perspectiva foram apontados diversos procedimentos visando diagnosticar e estabelecer uma estratégia de ação que sirva de orientação para gerir os riscos, bem como algumas formas de atuação para efetiva proteção, nesse contexto de planejamento e implementação de medidas de Contrainteligência no escopo da proteção de pessoas e Informações na Administração Pública.

## REFERÊNCIAS

BRASIL. Superior Tribunal Federal. INSTRUÇÃO NORMATIVA STJ/GP N. 12 DE 6 DE MAIO DE 2019. Disponível em: < https://ww2.stj.jus.br/processo/dj/documento/?seq_documento=21701701&data_pesquisa=08/05/2019&seq_publicacao=15760&versao=impressao&nu_seguimento=00001&parametro=null>. Acesso em: 16 abr. 2020 a.

BRASIL. Superior Tribunal Federal. Plano de Segurança Institucional do Ministério Público Federal. PORTARIA PGR/MPF N. 417 DE 5 DE JULHO DE 2013. Disponível em: < bibliotecadigital.mpf.mp.br>. Acesso em: 30 abr. 2020.

_____. COMISSÃO NACIONAL DE ENERGIA NUCLEAR. PORTARIA CNEN-PR Nº 012, DE 23 DE MARÇO DE 2018. Disponível em: < http://www.cnen.gov.br/images/cnen/documentos/acesso_a_informacao/Port-CNEN-PR-012-2018.pdf>. Acesso em: 5 fev. 2020 b.

_____. Exército. Comando de Operações Terrestres. Portaria n. 076 COTER, de 09 de julho de 2019. Manual de Campanha EB70-MC-10.220 – Contrainteligência. **Boletim do Exército**, Brasília, DF, n. 30, 26 de jul de 2019 c.

CHIAVENATO, Idalberto. Gestão de Pessoas. 4ªed. Rio de Janeiro. Manole, 2014.

DANTAS FILHO, Diógenes; Segurança e Planejamento. 1. ed. Rio de Janeiro: Ciência Moderna, 2004.

M. BISHOP, *Computer Security: Art and Science*, Addison Wesley, 2003.

MACÊDO, Diego. Ativos de informação e segurança em recursos humanos. Disponível em: <http://www.diegomacedo.com.br/ativos-de-informacao-e-seguranca-em-recursos-umanos/>**.** Acesso em 28 de agosto de 2020.

GHODDOSI, Nader. Gestão da Segurança da Informação. UNIASSELVI, 2016.

OLIVEIRA, Gercina Alves de; SILVA, Márcia Costa Alves da. Gestão de pessoas no setor público. UNIASSELVI, 2016.

PARANÁ. Polícia Civil do Paraná. Disponível em: < http://www.aipc.policiacivil.pr.gov.br/modules/conteudo/conteudo.php?conteudo=13>. Acesso em: 10 abr. 2020.

PADILHA, André Luiz Ferreira. Recursos Humanos. Uma poderosa ferramenta para a segurança corporativa. Disponível em: <https://administradores.com.br/artigos/recursos-humanos-uma-poderosa-ferramenta-para-a-seguranca-corporativa>. Acesso em 23 de agosto de 2020.