



Poder Judiciário

*Conselho Nacional de Justiça*

**ANEXO VII – Manual de Referência – Política de educação e cultura  
em segurança cibernética do Poder Judiciário**

# **Manual de Referência**

**Política de Educação e Cultura em Segurança Cibernética  
do Poder Judiciário**

Material de referência com as principais diretrizes necessárias para implantação da  
política de educação e cultura em segurança cibernética do Poder Judiciário



Poder Judiciário

*Conselho Nacional de Justiça*

## Sumário

Introdução .....	3
1. Disposições Gerais .....	3
1.1 Finalidade .....	3
1.2 Objetivo .....	4
1.3 Abrangência .....	4
1.4 Público-alvo .....	5
2. Programa de Capacitação em Segurança Cibernética do Poder Judiciário (PCASC-PJ).....	5
2.1 Tipo de Ações .....	5
2.2 Temas abrangidos.....	7
3. Competências para Implementação das Ações .....	7
3.1 Escolas de Formação.....	7
3.2 Área de Gestão de Pessoas .....	8
3.3 Área de Comunicação Social e Institucional.....	8
4. Resultados previstos .....	8



## Poder Judiciário

# *Conselho Nacional de Justiça*

### **Introdução**

0.1. Esta política visa estabelecer as diretrizes necessárias consubstanciadas em ações permanentes de capacitação, de educação, de engenharia social e de formação de cultura especializada que constituem fatores indispensáveis para a efetividade de ações de segurança cibernética.

0.2. O tema formação de cultura e de educação em segurança cibernética deve ser tratado de forma equânime, uniforme e articulado com todos os órgãos do Poder Judiciário e em conformidade com os mais atualizados paradigmas, procedimentos e padrões nacionais e internacionais.

0.3. É importante ressaltar a necessidade de ações constantes de formação de cultura, de educação, de atualização tecnológica e de reciclagem e atualização técnica no tema da segurança cibernética, que devem ser desenvolvidas de forma colaborativa entre os órgãos do Poder Judiciário, além de envolvimento multissetorial de instituições de ensino, pesquisa e fomento.

0.4. Vale destacar a diversidade e a multiplicidade de opções de cursos; programas de treinamento; modalidades de aquisição e disseminação de conhecimentos; formação técnica e gerencial; e plataformas tecnológicas educacionais presentes no mercado educacional contemporâneo, que devem pautar as ações a serem desenvolvidas por todos os órgãos do Poder Judiciário.

## **1. Disposições Gerais**

### **1.1 Finalidade**

1.1.1. A PCECSC-PJ tem a finalidade de desenvolver e fortalecer a cultura, a educação, a conscientização e as habilidades em segurança cibernética dos usuários de Tecnologia da Informação e Comunicação (TIC) e de Segurança da Informação (SI), bem como fomentar o desenvolvimento, o aprimoramento e a disseminação de conhecimentos, pesquisas e inovações dos profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação.



Poder Judiciário  
*Conselho Nacional de Justiça*

## 1.2 Objetivos

### 1.2.1. São objetivos da PCECSC-PJ:

- a) propiciar o constante aprimoramento dos níveis de segurança cibernética nos ativos e serviços de Tecnologia da Informação e Comunicação nos órgãos do Poder Judiciário;
- b) inserir o tema da segurança cibernética como tópico estratégico e primordial a constar das pautas institucionais de todos os órgãos do Poder Judiciário;
- c) promover a elevação do grau de conhecimento e de consciência quanto à cultura da segurança da cibernética no âmbito do Poder Judiciário;
- d) assegurar que todo usuário dos serviços de informação do Poder Judiciário tenha a devida compreensão de suas responsabilidades na proteção das informações dos órgãos do Poder Judiciário;
- e) assegurar que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos profissionais das áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação, em nível acadêmico, técnico, gerencial, entre outros aplicáveis.

## 1.3 Abrangência

### 1.3.1. Para os fins do disposto na PCECSC-PJ, a segurança cibernética abrange:

- a) a segurança da informação de forma geral;
- b) a segurança física e a proteção de dados pessoais e institucionais;
- c) a segurança física e a proteção de ativos de tecnologia da informação de forma geral;
- d) as ações destinadas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade de dados e informações;
- e) as ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade da prestação jurisdicional e administrativa dos órgãos do Poder Judiciário;
- f) as ações de planejamento, sistematização e normatização sobre temas atinentes à segurança cibernética;



## Poder Judiciário

### *Conselho Nacional de Justiça*

- g) as ações de comunicação, conscientização, formação de cultura e direcionamento institucional com vistas à segurança cibernética;
- h) as ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de Tecnologia da Informação e Comunicação que atuam na área de segurança cibernética.

#### **1.4 Público-alvo**

1.4.1. A PCESC-PJ deve ser aplicada a todos os usuários internos do Poder Judiciário, a saber:

- a) Magistrados e magistradas;
- b) Servidores e servidoras;
- c) Estagiários e estagiárias;
- d) Terceirizados e terceirizadas; e
- e) Colaboradores em geral.

## **2. Programa de Capacitação em Segurança Cibernética do Poder Judiciário (PCASC-PJ)**

### **2.1 Tipo de Ações**

2.1.1. Os órgãos do Poder Judiciário deverão desenvolver ações de capacitação, formação, reciclagem, fomento e conscientização em segurança cibernética, podendo incluir, entre outras:

- a) programas de formação;
- b) programas de reciclagem;
- c) programas de extensão educacional;
- d) programas de pesquisa e fomento de natureza técnica, acadêmica e científica;
- e) elaboração de artigos, materiais e publicações de natureza técnica, acadêmica e científica;
- f) programas de intercâmbio, imersão e cooperação educacional;
- g) ações periódicas de capacitação;
- h) cursos em plataformas do tipo *MOOC – Massive Open On-line Courses*;
- i) programas de certificação especializada;



## Poder Judiciário

### *Conselho Nacional de Justiça*

- j) palestras, congressos, seminários e afins;
- k) concursos, competições e premiações; e
- l) *workshops*.

2.1.2. Além das ações direcionadas para públicos-alvo específicos os órgãos do Poder Judiciário devem estabelecer concomitantemente as seguintes ações de alcance amplo:

- a) campanhas;
- b) produção de pôsteres, cartazes, folhetos, notas informativas e/ou boletins periódicos;
- c) testes públicos de segurança.

2.1.3. Cada órgão do Poder Judiciário deverá estabelecer uma carga horária mínima de capacitação não superior a 1 (um) ano, podendo as ações previstas neste Manual serem efetuadas em diversas cargas horárias e níveis de formação, assim divididas:

- a) ações de capacitação em geral;
- b) cursos de educação executiva de curta duração;
- c) cursos de graduação;
- d) cursos de especialização;
- e) cursos de mestrado;
- f) cursos de doutorado; e
- g) cursos de pós-doutorado.

2.1.4. As ações previstas neste Manual deverão ser priorizadas no formato considerado mais efetivo em termos de adequação ao aprendizado, ao aproveitamento e aos objetivos pretendidos, podendo ser realizada, em âmbito nacional ou internacional, nas seguintes modalidades:

- a) presencial;
- b) telepresencial;
- c) *on-line*; ou
- d) híbrida.



## Poder Judiciário

# *Conselho Nacional de Justiça*

## **2.2 Temas abrangidos**

2.2.1. Para efeitos deste Manual, os seguintes temas devem ser contemplados obrigatoriamente, além de outros:

- a) governança e gestão de segurança cibernética;
- b) elaboração de políticas institucionais de segurança cibernética;
- c) tratamento de incidentes de segurança cibernética;
- d) forense computacional;
- e) inteligência e investigação em crimes cibernéticos;
- f) gerenciamento de identidades, acesso e privilégios;
- g) segurança no desenvolvimento de *software*;
- h) gestão de continuidade de negócios;
- i) gestão de riscos de TIC e SI;
- j) auditoria e conformidade de sistemas de informação;
- k) segurança em computação em nuvem;
- l) segurança em aplicações móveis; e
- m) segurança em redes sociais.

## **3. Competências para Implementação das Ações**

### **3.1. Escolas de Formação**

3.1.1. Compete às Escolas de Formação, aos Centros de Educação e Capacitação e às demais unidades administrativas responsáveis pela capacitação de magistrados e magistradas e de servidores e servidoras do Poder Judiciário:

- a) adotar medidas para a concretização da PCESC-PJ descrita neste Manual.
- b) elaborar Programas de Formação, Capacitação e Reciclagem de magistrados e magistradas e de servidores e servidoras que descrevam, com previsão bianual e de forma detalhada, as ações a serem realizadas, as metas a serem atingidas, os quantitativos previstos, os critérios de participação e a contabilização de horas, entre outros elementos que evidenciem o cumprimento dos itens previstos neste Manual.
- c) propor celebração de parcerias, de acordos de cooperação técnica, de convênios, entre outros instrumentos afins, tanto em âmbito nacional como



## Poder Judiciário

### *Conselho Nacional de Justiça*

internacional, com instituições multissetoriais, a fim de maximizar os resultados descritos como objetivos deste Manual;

d) atuar de forma coordenada com outros órgãos do Poder Judiciário e de outros Poderes com vistas ao oferecimento mútuo de vagas, ao compartilhamento de capacitações, à troca materiais e de experiências, à organização conjunta de eventos e de treinamentos, ao compartilhamento de ações de instrutoria interna, entre outras ações afins, para a máxima efetividade dos objetivos previstos neste Manual.

#### **3.2 Área de Gestão de Pessoas**

3.2.1. É responsabilidade da área de gestão de Pessoas de cada órgão do Poder Judiciário a adoção de procedimentos, normativos e práticas administrativas que viabilizem a inscrição, a participação e o pagamento de ações de capacitação previstas neste Manual, principalmente no caso de formas diversas de pagamento, tais como cartões de crédito, boletos bancários, meios eletrônicos de pagamento, entre outras.

3.2.2. Os normativos e procedimentos previstos poderão incluir regras, procedimentos, critérios e condições para o pagamento prévio por parte do participante e posterior ressarcimento, integral ou parcial, por parte do órgão.

#### **3.3 Área de Comunicação Social e Institucional**

3.3.1. Compete às áreas de Comunicação Social e Institucional dos órgãos do Poder Judiciário, incluírem, em seus planejamentos anuais, programas de divulgação, conscientização, informação e esclarecimentos aos seus públicos-alvo, tanto internos como externos, referentes a temas de Segurança Cibernética.

## **4 Resultados previstos**

4.1. Os programas de formação, capacitação e reciclagem deverão propiciar que os órgãos do Poder Judiciário possuam:





## Poder Judiciário

### *Conselho Nacional de Justiça*

- a) profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação em seus quadros, qualificados em segurança cibernética em nível de graduação, pós-graduação ou de certificações especializadas;
- b) todos os usuários internos com educação básica e cultura em segurança cibernética.

4.2. Os órgãos do Poder Judiciário deverão apresentar ao CNJ, no início do ano seguinte, relatório que comprove a efetividade das ações realizadas no exercício anterior e o respectivo desempenho dos usuários e profissionais treinados.