**Centro Universitário de Brasília**
**Instituto CEUB de Pesquisa e Desenvolvimento - ICPD**

**LUIS GUSTAVO LOYOLA DOS SANTOS FILHO**

# ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS TRIBUNAIS SUPERIORES DO PODER JUDICIÁRIO BRASILEIRO

Brasília
2016

**LUIS GUSTAVO LOYOLA DOS SANTOS FILHO**

# ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS TRIBUNAIS SUPERIORES DO PODER JUDICIÁRIO BRASILEIRO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília
2016

**LUIS GUSTAVO LOYOLA DOS SANTOS FILHO**

# ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS TRIBUNAIS SUPERIORES DO PODER JUDICIÁRIO BRASILEIRO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília, ___ de _____ de 2016.

**Banca Examinadora**

_____

Prof. Dr. Maurício da Rocha Lyra

_____

Prof. Dr. Paulo Rogério Foina

_____

Prof. Dra. Tânia Cristina da Silva Cruz

Agradeço primeiramente a Deus pelo dom da vida e por iluminar o meu caminho durante esta jornada. Aos meus pais Vera Lúcia e Luís Gustavo e minhas irmãs Patrícia, Eliana e Vânia por sempre me incentivarem e acreditarem no meu potencial. A minha esposa Priscilla, que com muito carinho e dedicação se sacrificou para que eu pudesse concluir mais esse desafio, amo nossa parceria. Aos meus filhos Alexandre e Isabela por entenderem que a ausência do papai em alguns momentos não foi em vão. Por fim, ao meu orientador Maurício Lyra por me ajudar a lapidar este trabalho e torná-lo um instrumento de melhoria para a nossa sociedade.

## RESUMO

Derivada da Governança Corporativa, a Governança da TI surge para apoiar as empresas e/ou órgãos de governo que necessitam gerir suas arquiteturas de informação desde a infraestrutura passando pelo sistemas e processos alinhado diretamente com as estratégias corporativas. A segurança da informação tem um papel fundamental nessa gestão e a política de segurança da informação é o instrumento que permite que o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação seja estabelecido e divulgado a toda corporação. Este trabalho teve por finalidade verificar o nível de maturidade das políticas de segurança da informação dos tribunais superiores do judiciário brasileiro, identificando sua aderência às melhores práticas, baseado em uma metodologia desenvolvida e aplicada em outro estudo visando análise de políticas de segurança da informação dos órgãos do Poder Executivo. A metodologia baseia-se em uma análise quantitativa relacionada a quantidade de requisitos considerados como essenciais para elaboração de uma Política de Segurança da Informação e que foram identificados em cada uma da Políticas analisadas. Os resultados obtidos indicam que a maturidade das Políticas de Segurança dos Tribunais carece de maior atenção no sentido de se buscar o seu aperfeiçoamento visando aumento na efetividade do cumprimento das políticas, que tratam o tema Segurança da Informação, em cada um dos órgãos analisados.



**Palavras-chave**: Segurança da Informação. Política da Segurança da Informação. Normas e Padrões de Segurança. Governança em Tecnologia da Informação.

## ABSTRACT

Derived from the Corporate Governance, the IT Governance comes to support companies and / or government agencies who need to manage their information architectures from infrastructure through the systems and processes aligned directly with corporate strategies. Information security plays a key role in management and information security policy is the instrument that allows the set of standards, methods and procedures used for information security maintenance is established and disclosed the whole corporation. This work aimed to verify the level of maturity of information security policies of the top Brazilian judicial courts, identifying their adherence to best practices, based on a methodology developed and applied in another study to analyze security policy information organs the executive branch. The methodology is based on a quantitative analysis related to quantity requirements considered essential for the preparation of an Information Security Policy and that have been identified in each of the analyzed policies. The results indicate that the maturity of the security policies of the courts needs further attention in order to seek its improvement aimed at increasing the effectiveness of compliance with policies that address the topic Information Security, in each of the organs analyzed.



**Key words**: Information Security. Information Security Policy. Standards and Security.Governance in Information Technology.

## LISTA DE FIGURAS

## LISTA DE TABELAS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| PSIC | Política de Segurança da Informação |
| SGSI | Sistema de Gestão da Segurança da Informação |
| SI | Segurança da Informação |
| TCU | Tribunal de Contas da União |
| IBGC | Instituto Brasileiro de Governança Corporativa |
| STF | Supremo Tribunal Federal |
| STJ | Superior Tribunal de Justiça |
| TST | Tribunal Superior do Trabalho |
| TSE | Tribunal Superior Eleitoral |
| STM | Superior Tribunal Militar |

**SUMÁRIO**

# INTRODUÇÃO

As transformações vividas pelas organizações vêm consolidando a informação como o principal ativo estratégico de uma empresa ao possibilitar o aumento da sua competitividade e a possibilidade de assumir um posicionamento estratégico onde as decisões rápidas e corretas são fundamentais para se atingir resultados satisfatórios. Para se atingir esse patamar, a tomada de decisão deve estar baseada no maior número de informações e conhecimentos.

Soma-se a esse cenário, os avanços tecnológicos que o mundo tem vivido nas últimas décadas, é nítido que para o funcionamento estratégico, tático e operacional de qualquer empresa, que almeja o sucesso, o investimento em tecnologias com destaque para os sistemas de informação.

Nos anos 90, em um movimento que ocorreu com mais intensidade nas grandes empresas dos Estados Unidos, os acionistas, sentiram a necessidade de implementarem regras que os assegurassem contra abusos da diretoria ou falhas na atuação do conselho de administração no que diz respeito às decisões estratégicas que direcionavam o rumo dos negócios.

A esse conjunto de regras damos o nome de Governança Corporativa que se baseia em quatro princípios básicos: Transparência (disclosure), Equidade (fairness), Prestação de Contas (accountability) e Respeito ao cumprimento das leis (compliance), segundo o IBGC.

Derivada da Governança Corporativa, surge a necessidade de as empresas gerirem suas arquiteturas de informação desde a infraestrutura, passando pelos sistemas e processos, e mais, que tudo isso permaneça alinhado e sustentando as estratégias da corporação. Nesse cenário, nasce o conceito da Governança de TI.

Atualmente existem inúmeros frameworks, normas e guias de melhores práticas que podem auxiliar na implementação da Governança de TI. Neste trabalho, abordaremos os aspectos de Segurança da Informação, por meio de um estudo sobre a política de segurança da informação nos tribunais superiores do judiciário

brasileiro, assunto de grande relevância na elaboração das políticas de Governança de TI destes órgãos.

Cientes da necessidade e da importância de uma política de segurança da informação, ainda mais quando se trata de informações de governo onde a soberania do país pode estar em jogo, o governo brasileiro, por meio do decreto nº 3.505, de 13 de junho de 2000, instituiu a política nacional de segurança da informação, que determinou a todos os órgãos entidades da Administração Pública Federal, direta e indireta, elaborem e mantenham sua Política de Segurança da Informação.

Com o objetivo de verificar o nível de maturidade das Políticas de Segurança da Informação dos órgãos da administração pública federal direta é que Ferrer e Lyra (2014) desenvolveram o trabalho *Análise da maturidade da política de segurança da informação dos órgãos da administração pública federal direta*.

O presente estudo, se propõe, baseado na metodologia desenvolvida por Ferrer e Lyra (2014), expandir a análise das políticas de segurança da informação para o poder judiciário brasileiro, especificamente nas políticas de segurança dos tribunais superiores.

Deste objetivo, outros mais específicos serão concluídos: identificar a aderência das Políticas às melhores práticas, realizar uma análise de maturidade e comparar os resultados obtidos no presente trabalho com a análise de Ferrer e Lyra (2014) .

Para alcançar esses objetivos, procedeu-se da seguinte maneira: inicialmente, foi feita pesquisa bibliográfica em artigos científicos e em livros técnicos especializados que tratam do assunto de Segurança da Informação datados entre 2003 e 2015. Realizou-se uma pesquisa na web pelas PSIC de todos os tribunais superiores do judiciário brasileiro, com o intuito de realizar uma análise comparativa entre as PSIC e as melhores práticas definidas por Ferrer e Lyra (2014). Por fim, realizou-se uma análise crítica e comparativa de forma a apresentarmos uma matriz com o nível de maturidade das PSIC dos tribunais analisados, assim como uma análise destas PSIC.

A justificativa para o presente trabalho é ampliar o conhecimento sobre a maturidade das políticas de segurança da informação iniciada por Ferrer e Lyra

(2014), buscando demonstrar a importância que o poder judiciário brasileiro tem dado ao assunto além de poder colaborar com a identificação de pontos de melhoria na eficiência e eficácia das políticas de segurança da informação analisadas.

O presente trabalho foi então estruturado em 4 capítulos.

No primeiro capítulo, apresenta-se um referencial teórico com conceitos relacionados à segurança da informação presentes na norma ISO 27.002; o segundo capítulo discorre sobre os conceitos relacionados à Política de Segurança da Informação; o terceiro capítulo detalha os procedimentos metodológicos adotados na elaboração da análise das PSIC, descrevendo brevemente o trabalho de análise realizado por Ferrer e Lyra (2014) sobre as PSIC do poder executivo; o quarto e último capítulo proporciona uma análise sobre os resultados alcançados apresentando uma análise das PSIC do poder judiciário e indicando o seu nível de maturidade, além de um comparativo entre os poderes executivo e judiciário no que diz respeito às suas políticas de segurança da informação; por fim, apresenta-se as conclusões sobre a pesquisa realizada.

# 1 SEGURANÇA DA INFORMAÇÂO

Para Beal (2008), a segurança da informação visa preservar ativos de informação, levando em conta três objetivos fundamentais: Confidencialidade, Integridade e Disponibilidade.

> Para Manoel (2014, p.4), os requisitos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade representam os princípios básicos que, atualmente, orientam a análise, o planejamento, a implantação e controle da Segurança da Informação para um determinado grupo de informações que se deseja proteger.

Sêmola (2003, p.43) define segurança da informação como sendo “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

## *1.1* Objetivos Fundamentais da Segurança da Informação

### 1.1.1 *Confidencialidade*

Beal (2008) define confidencialidade como sendo a “garantia de que o acesso à informação é restrito aos seus usuários legítimos”.

> Para Dantas (2011, p.14), ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

### 1.1.2 *Disponibilidade*

Dantas (2011, p.12) define quebra da disponibilidade quando a informação não está disponível no momento em que um usuário ou o destinatário da informação deseja utilizá-la.

Disponibilidade é toda a informação gerada ou adquirida e que deve estar disponível ao seu usuário no momento em que necessitem para qualquer finalidade, por Sêmola (2003, p.45).

### 1.1.3 *Integridade*

Beal (2008) define que integridade visa a “garantia da criação legitima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações”.

Já para Dantas (2011, p.11) garantir a integridade é “permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente”.

## 1.2 A informação como um ativo

Para Sêmola (2003, p.45), informação é um conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos. Ele acrescenta ainda que a informação pode ser manipulada por inúmeros elementos do processo, ao qual damos o nome de ativos, os quais são alvo de proteção da segurança da informação.

> Para o TCU (2012), informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

Dantas (2011, p.21) nos apresenta a definição clássica de ativo como sendo um conjunto de bens e direitos de uma entidade e atualmente ativo é tido como tudo aquilo que possui valor para a empresa.

## 1.3 Ameaças e vulnerabilidades à informação

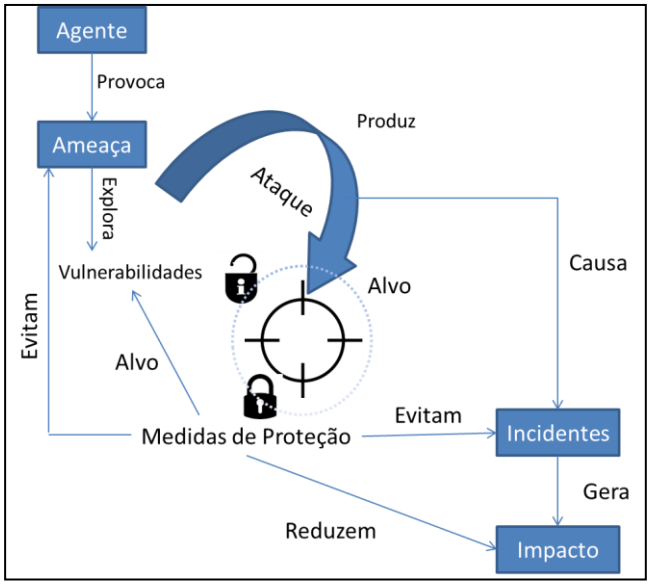
Para Fontes (2008), roubo de informações sempre existiu e existirá. As organizações precisam estar atentas continuamente para proteger um dos bens mais importantes para o negócio: a informação.

As vulnerabilidades são fragilidades presentes ou associadas a ativos de informação, que, ao serem exploradas, permitem a ocorrência de incidente na segurança da informação, por Sêmola (2003, p.48).

Para Lyra (2008, p.6), ameaça trata-se de um ataque potencial a um ativo da informação. Um agente que se aproveita de vulnerabilidades para quebrar um dos objetivos fundamentais da segurança da informação.

> Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (tais como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitarem das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos (ISO 27002:2013).

**Figura 1** – Ameaça, vulnerabilidade e o risco para segurança da informação.




**Fonte**: Beal (2008, p. 16) (adaptado)

## 1.4 Norma ABNT NBR ISO/IEC 27002

Segundo a ISO 27002:2013, a norma foi projetada para que fosse utilizada por organizações como uma referência, na escolha de controles para implementação de controles de segurança da informação, baseado na ABNT NBR ISO/IEC 27001 e amplamente adotado pelas organizações.

Para Ferrer e Lyra (2014), a descrição dos controles preventivos, em sua grande maioria, evita a ocorrência de incidentes envolvendo as informações corporativas, visando reduzir o tempo de exposição ao risco, que permitem detectar, de maneira mais rápida e efetiva, eventuais violações às regras do Sistema.

> Embora o conteúdo da PSIC possa variar de acordo com o tipo da instituição, o seu tamanho, área de atuação, cultura organizacional, missão, estágio de maturidade, grau de informatização, ativos informacionais críticos, entre outros aspectos, ela deverá abranger, sempre que cabível, o máximo de controles Ferrer e Lyra (2014).

A norma NBR ISO/IEC 27002:2013 está organizada em 14 (quatorze) seções de controle de segurança da informação, os quais serão apresentados abaixo, 35 objetivos de controle e 114 controles.

### 1.4.1 *Políticas de segurança da informação*

Segundo a norma NBR ISO/IEC 27002:2013, o objetivo de uma PSIC é criação de um documento capaz de prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

### 1.4.2 *Organização da segurança da informação*

O objetivo dessa seção, segundo a norma NBR ISO/IEC 27002:2013, é estabelecer uma estrutura para gerenciar a implementação da segurança da informação, já que as atividades de segurança devem ter representantes de toda a organização com funções e papéis estabelecidos e bem definidos.

### 1.4.3 *Segurança em recursos humanos*

A norma NBR ISO/IEC 27002:2013 preconiza que antes da contratação a organização deve se assegurar de que os funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados. Ela sugere, também, que haja uma preocupação da organização em manter os funcionários conscientes e cumprindo as suas responsabilidades no que tange a segurança da informação. Por fim, aponta a necessidade de se preocupar com a proteção dos interesses da organização durante o processo de mudanças ou encerramento de contratação.

### 1.4.4 *Gestão de ativos*

A norma NBR ISO/IEC 27002:2013 aconselha as organizações a identificarem quais são os seus ativos, definindo responsabilidades apropriadas para a proteção dos mesmos. Ela ainda defende que a informação seja classificada e receba um nível adequado de proteção de acordo com sua importância.

### 1.4.5 *Controle de acesso*

Segundo a norma NBR ISO/IEC 27002:2013, o acesso à informação, aos recursos de processamento das informações e aos processos de negócios devem ser controlados com base nos requisitos de negócio e na segurança da informação. Dessa forma, ela sugere que haja limitação no acesso à informação e aos recursos de processamento da informação assegurando acesso de usuário autorizado e prevenindo o acesso não autorizado a sistemas e serviços. A norma ainda destaca que os usuários devem sentir-se responsáveis pela proteção das suas informações de autenticação.

### 1.4.6 *Criptografia*

Para a norma NBR ISO/IEC 27002:2013, a utilização de controles criptográficos assegura o uso efetivo e adequado da criptografia para proteger a confidencialidade e integridade da informação. Nesse cenário, a norma alerta para a importância em considerar as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas.

### 1.4.7 *Segurança física e do ambiente*

Em relação à segurança do ambiente, a norma NBR ISO/IEC 27002:2013 orienta que os locais onde haja instalações para o processamento das informações críticas ou sensíveis devem estar em áreas seguras, com controles de acesso apropriados, incluído a proteção física dos equipamentos impedindo perdas, danos, furto ou comprometimento de ativos e interrupção das atividades do processo produtivo da organização.

### 1.4.8 *Segurança nas operações*

Segundo a norma NBR ISO/IEC 27002:2013, é importante garantir a operação segura e correta dos recursos de processamento da informação, assegurando que recurso e informação estejam protegidos contra códigos maliciosos e perda de dados. Sob a ótica do monitoramento, a norma preconiza o registro de eventos e a preocupação em se gerar evidências. Ela ainda abrange a necessidade de se assegurar a integridade dos sistemas operacionais bem como a prevenção da exploração de vulnerabilidades técnicas. Por fim, sugere que as auditorias de sistemas de informação devem sempre buscar minimizar os impactos nos sistemas operacionais.

### 1.4.9 *Segurança nas comunicações*

Com relação à segurança nas comunicações, a norma NBR ISO/IEC 27002:2013 orienta para que se garanta a proteção das informações em rede e dos recursos de processamento que os apoiam. A manutenção da segurança da informação deve acontecer tanto para as informações transferidas internamente quanto com qualquer entidade externa da organização.

### 1.4.10 *Aquisição, desenvolvimento e manutenção de sistemas*

A norma NBR ISO/IEC 27002:2013, sugere que a organização considere garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação incluindo requisitos para SI que fornecem serviços sobre redes públicas. A norma sugere ainda que a SI esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de Informação inclusive na proteção dos dados que são usados para testes.

### 1.4.11 *Relacionamento na cadeia de suprimento*

A norma NBR ISO/IEC 27002:2013, diz que é importante manter o relacionamento na cadeia de suprimento para se garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores mantendo um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

### 1.4.12 *Gestão de incidentes de segurança da informação*

A norma NBR ISO/IEC 27002:2013, recomenda que seja assegurado um enfoque consistente e efetivo no gerenciamento dos incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

### 1.4.13 *Aspectos da segurança da informação na gestão da continuidade do negócio*

A norma NBR ISO/IEC 27002:2013, sugere que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização assegurando a disponibilidade dos recursos de processamento da informação.

### 1.4.14 *Conformidade*

Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança garantindo que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização é o que recomenda a norma NBR ISO/IEC 27002:2013.

# 2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para Ferreira e Araújo (2006, p.9), a Política de Segurança é definida como sendo um conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação. Eles complementam dizendo que tudo deve ser formalizado e divulgado a todos os usuários que fazem uso dos ativos de informação.

> Para Sêmola (2003, p.105), é a Política de Segurança que estabelece padrões, responsabilidades, e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada.

A norma NBR ISO/IEC 27002:2013 diz que a Política de Segurança da Informação tem por objetivo prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Ferreira e Araújo (2006, p.10) defendem que a Política deve expressar os anseios dos proprietários ou acionistas, que são responsáveis por decidir os destinos de todos os recursos da organização em relação ao uso da informação.

> “É notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada junto aos funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais”, Sêmola (2003, p.105).

Para Dantas (2011, p.131), a Política é a materialização da intenção do que se deseja fazer transformando em princípios, valores, compromissos, requisitos, objetivos e orientações sobre o que deve ser feito a fim de alcançar um padrão de proteção para as informações.

Para Ferreira e Araújo (2006, p.11) as políticas, normas e procedimentos de segurança da informação devem ser simples, compreensíveis, homologadas e assinadas pela Alta Administração, estruturadas de forma a permitir a sua implantação por fases, alinhadas com as estratégias de negócio da empresa, padrões e procedimentos já existentes, orientadas aos riscos, flexíveis, protetores dos ativos de informações e positivas e não apenas concentradas em ações proibitivas ou punitivas.

## 2.1 Tipos de Políticas de Segurança da Informação

Para Fontes (2012, p.77), o conjunto da política de segurança da informação deve ter uma arquitetura que facilite a estruturação desses regulamentos. Diz também que não existe uma estrutura rígida de separação dos tipos de orientações.

Ferreira (2003, p.34), nos apresenta 3 tipos de políticas:

> a) Políticas do tipo Regulatórias: São implementadas devido às necessidades legais que são impostas à organização. Normalmente, são muito específicas para um tipo de ramo de atividade. Assegurar que a organização está seguindo os procedimentos e prover conforto à organização na execução de suas atividades, pois certamente estão seguindo os requisitos legais são características marcantes para a aplicação desse tipo de política.
>
> b) Políticas do tipo Consultivas: Sugerem a busca por uma conscientização dos funcionários da organização a adotar as suas recomendações como se fossem obrigatórias. Sugere, bem diretamente, quais ações ou métodos devem ser utilizados para a realização de uma determinada tarefa/atividade.
>
> c) Políticas do tipo Informativas: Possui um caráter apenas informativo. Nenhuma ação é desejada e não existem riscos, caso não seja cumprida. Embora não seja tão rigorosa quanto à regulatória e à consultiva, pode contemplar uma série de observações importantes, bem como advertências severas.

## 2.2 Etapas para o desenvolvimento de uma Política de Segurança da Informação

Para Ferreira e Araújo (2006, p.12-14), o desenvolvimento e a implantação das políticas, normas e procedimentos de segurança da informação são, geralmente, divididos em 4 fases:

> a) Fase I – Levantamento de Informações: Nessa fase é feito um levantamento dos padrões, normas e procedimentos de segurança já existentes para análise. Realiza-se um entendimento das necessidades e uso dos recursos da tecnologia nos processos de negócio. Buscam-se informações sobre o ambiente de negócios (Processos, Tendências de mercado, Controles e áreas de risco). Por fim, obtêm-se informações sobre o ambiente tecnológico da organização (Workflow entre ambientes, redes, plataformas).
>
> b) Fase II – Desenvolvimento do Conteúdo das Políticas e Normas de Segurança: Nessa fase realiza-se um gerenciamento da política de segurança abrangendo a definição da segurança da informação, o objetivo do gerenciamento, fatores críticos de sucesso, gerenciamento da versão e manutenção da política e a referencia para outras políticas, padrões e procedimentos. É nesse momento que se atribui regras e responsabilidades para o comitê de segurança da informação, aos proprietários das informações, das áreas de segurança da informação, dos usuários das informações e da Auditoria interna.

> Durante essa fase é que se definem os critérios para classificação das informações com seus níveis, mecanismos de reclassificação, procedimentos de Armazenamento e descarte.
>
> Por fim, são desenvolvidos os procedimentos de segurança de informações contendo por exemplo: Uso de Internet, uso de correio eletrônico, manutenção de teste e equipamentos, backup, controle de acesso físico entre outros.
>
> c) Fase III – Elaboração dos procedimentos de segurança da Informação: Nessa fase é realizada a pesquisa sobre as melhores práticas em segurança da informação utilizadas no mercado, possibilitando o desenvolvimento de procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização. Por fim, formaliza-se os procedimentos para integrá-los às políticas corporativas.
>
> d) Fase IV – Revisão, Aprovação e Implantação das Políticas, Normas e Procedimentos de Segurança da Informação: Nessa última fase, realiza-se a revisão e aprovação das políticas, normas e procedimentos de segurança da informação, efetiva a sua implantação atuando na divulgação das responsabilidades dos colaboradores, bem como da importância das políticas, normas e procedimentos de segurança. Essa divulgação pode ser feita por comunicados corporativos, palestras e com a preparação de material para consulta.

## 2.3 Fatores Comuns entre as Políticas de Segurança da Informação

A norma NBR ISO/IEC 27002:2013, sugere que no mais alto nível a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Sugere-se na norma NBR ISO/IEC 27002:2013, que as políticas de segurança da informação possam contemplar requisitos oriundos da:

a) estratégia do negócio;

b) de regulamentações, legislação e contratos;

c) do ambiente de ameaça da segurança da informação, atual e futuro.

É conveniente, segundo a norma NBR ISO/IEC 27002:2013, que a política de segurança da informação contenha declarações relativas a:

a) definição da segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;

b) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;

c) processos para o tratamento dos desvios e exceções.

> No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos, conforme a norma NBR ISO/IEC 27002:2013.

De acordo com Ferreira e Araújo (2006, p.15 a 17), todas as políticas bem elaboradas, geralmente, possuem os mesmos conceitos. Algumas são mais severas e outras mais sutis. Independentemente deste tipo de característica, quase todas contemplam os seguintes aspectos:

> a) Especificação da política: Deve ser breve, utilizar palavras simples e formalizar o que é esperado dos funcionários da organização. Deve fornecer aos leitores informações suficientes para saber se os procedimentos descritos na política são aplicáveis a eles ou não.
>
> b) Declaração da Alta Administração: Um dos itens mais importantes é o nome do executivo principal da organização, atestando sua divulgação e exigindo sua utilização. Isso demonstra aos colaboradores que ele está de acordo com as políticas expostas.
>
> c) Autores / patrocinadores da política: Nomes dos Profissionais ou equipes que desenvolveram as políticas devem estar especificados no documento para que qualquer dúvida de interpretação ou sugestões de mudanças possam ser diretamente enviadas aos autores.
>
> d) Referências a outras políticas, normas e procedimentos: É comum que as políticas em vigor façam referência a outros regulamentos internos já existentes ou em desenvolvimento.
>
> e) Procedimentos para requisição de exceções à política: A requisição de exceções à política é importante e geralmente se divulga os procedimentos para a sua solicitação e não quais as condições as exceções serão concedidas.
>
> f) Procedimentos para mudanças da política: Muitas organizações não atualizam suas políticas. Atualmente, devido à alta rotatividade de profissionais nas empresas, as políticas devem especificar responsáveis, em nível hierárquico e/ou especialização técnica, para seu controle e atualização.
>
> g) Datas de publicação, validade e revisão: A política deve possuir a assinatura do principal executivo aprovando-a, a data da última atualização e do início de sua vigência. Estas informações são importantes, pois ajudam a controlar suas revisões e atualizações periódicas.

## 2.4 Características e Benefícios

Beal (2008, p.49) alerta que os esforços de elaboração, aprovação, manutenção e divulgação da PSI não são suficientes para assegurar o cumprimento das diretrizes de segurança definidas pela organização. A garantia de conformidade com a politica de segurança depende ainda de uma avaliação periódica do

comportamento de todos os envolvidos na implementação dos controles, de modo que eventuais desvios em relação às diretrizes estabelecidas possam ser identificados e corrigidos.

> Os benefícios da segurança da informação estão na prevenção de perdas financeiras que a organização pode ter, no caso da ocorrência de incidentes de segurança da informação. A organização também pode abalar a sua imagem ou sofrer ações na justiça pelas perdas que seus sistemas possam causar aos seus clientes, e Abreu (2012, p.426).

Para Ferreira e Araújo (2006, p.18), para que a política seja efetiva deve ter algumas características como:

a) Ser verdadeira: Exprimir o pensamento da empresa e ser coerente com as ações da organização;

b) Ser complementada com a disponibilidade de recursos: Uma ação concreta de que a política é levada a sério pela direção é a liberação de recursos financeiros e de pessoal;

c) Ser válida para todos: Deve ser cumprida por todos os usuários que utilizam a informação da organização;

d) Ser simples: Deve ser de fácil leitura e compreensão;

e) Comprometimento da alta administração da organização: Deve ser assinada pelo mais alto executivo, explicitando assim, o seu total apoio à política.

Ferreira e Araújo (2006, p.19) classifica os principais benefícios alcançados com a implementação de uma política de segurança da informação em três categorias: Benefícios de curto, médio e longo prazo.

Como benefícios de curto prazo, Ferreira e Araújo (2006, p.19) destacam:

- Formalização e documentação dos procedimentos de segurança adotados pela empresa;
- Implementação de novos procedimentos e controles;
- Prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou desastres;
- Maior segurança nos processos do negócio.

Como benefícios de médio prazo, Ferreira e Araújo (2006, p.20) indicam:

- Padronização dos procedimentos de segurança incorporados na rotina da empresa;
- Adaptação segura de novos processos do negócio;

- Qualificação e quantificação dos sistemas de resposta a incidentes;
- Conformidade com padrões de segurança.

Como benefícios de longo prazo, Ferreira e Araújo (2006, p.20) apontam:

- Retorno sobre o investimento realizado, por meio da redução da incidência de problemas relacionados à segurança;
- Consolidação da imagem associada à Segurança da Informação.

# 3 PROCEDIMENTO METODOLÓGICO

Ferrer e Lyra (2014, p.36) realizaram uma análise da norma ABNT NBR ISO/IEC 27002:2013 e verificaram que os requisitos abaixo são imprescindíveis e necessários para a construção de uma política de segurança da informação e comunicação adequada:

1. Conter toda a regulamentação, legislação e contratos que a política dever estar amparada;
2. Conter uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco;
3. Contemplar o escopo da segurança da informação, conceitos, definições e a descrição da importância da Segurança da Informação;
4. Deve estar declarado os Princípios da segurança da informação;
5. Objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
6. Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
7. Processos para o tratamento dos desvios e exceções quando há violação na política de segurança da informação;
8. Processo de gestão de continuidade do negócio;
9. Políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos. (ex.: controle de acesso; classificação e tratamento da informação, etc.);
10. As políticas devem ser comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de um programa de conscientização, educação e treinamento em segurança da informação;

11. As políticas de segurança da informação devem ser analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia;

12. Deve haver a declaração do comprometimento da Direção apoiando as metas e princípios da organização.

A partir dos requisitos apresentados, Ferrer e Lyra (2014, p.38) elaboraram uma tabela contendo os requisitos necessários para uma política de segurança da informação e relacionaram os órgãos que tiveram suas políticas analisadas por eles.

O trabalho de Ferrer e Lyra (2014) se propôs a fazer uma análise do nível de maturidade das políticas de segurança da informação de um recorte de órgãos do poder executivo brasileiro, baseado nos 12 requisitos citados anteriormente.

Este trabalho será concebido nos mesmos moldes do trabalho de Ferrer e Lyra (2014), porém focando em um recorte de órgãos do poder judiciário brasileiro, mais especificamente dos tribunais superiores.

Segundo a Controladoria Geral da União, através do site “Acesso à Informação”, a Lei nº 12.527/2011, denominada Lei de Acesso à Informação, regulamenta o direito constitucional de acesso às informações públicas. Essa norma entrou em vigor em 16 de maio de 2012 e criou mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.

A lei vale para os três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Contas e Ministério Público.

Por meio da Lei de Acesso à Informação, foi solicitado aos tribunais superiores do judiciário brasileiro que apresentassem as suas respectivas políticas de segurança da informação.

A tabela 1 foi gerada a partir da adaptação da tabela existente no trabalho de Ferrer e Lyra (2014, p.38) apresentando cada um dos tribunais superiores do judiciário brasileiro, objeto desta análise.

**Tabela 1 - Requisitos de uma PSIC segundo a ISO 27002:2013**

| Requisitos necessários para uma PSIC segundo a ISO 27002:2013 | Supremo Tribunal Federal | Superior Tribunal de Justiça | Superior Tribunal Militar | Tribunal Superior do Trabalho | Tribunal Superior Eleitoral |
|---|---|---|---|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | | | | | |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | | | | | |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | | | | | |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | | | | | |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | | | | | |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | | | | | |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | | | | | |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | | | | | |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | | | | | |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | | | | | |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | | | | | |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | | | | | |

O passo seguinte será uma análise das políticas de cada tribunal superior baseado na tabela 1. Cada linha da tabela 1 será preenchida com “SIM”, caso seja identificado na PSIC do tribunal analisado o requisito referente a linha em questão. Caso contrário, será preenchido com “NÂO”.

Em seguida, as informações serão tabeladas para melhor apresentar os dados coletados. A análise dos dados nos permitirá estabelecer o grau de maturidade de cada uma das politicas analisadas.

Por fim, será feita uma comparação entre os resultados obtidos pelo trabalho de Ferrer e Lyra (2014) que teve foco no poder executivo e o presente trabalho com foco poder judiciário.

# 4 ANÁLISE DAS PSIC DOS TRIBUNAIS SUPERIORES DO JUDICIÁRIO BRASILEIRO

As políticas de segurança da informação, objeto desta análise, foram solicitadas e recebidas, por meio da lei de acesso à informação, em maio de 2015. Sendo assim, a análise que será apresentada neste trabalho reflete a situação das PSIC no referido período

Os tribunais superiores do judiciário brasileiro, cuja as políticas de segurança da informação serão objeto de análise são:

a) Supremo Tribunal Federal;

b) Superior Tribunal de Justiça;

c) Superior Tribunal Militar;

d) Tribunal Superior Eleitoral;

e) Tribunal Superior do Trabalho.

## 4.1 Mapeamento de requisitos das PSIC dos Tribunais

Assim como Ferrer e Lyra (2014), através da leitura das PSIC de cada tribunal superior foi possível identificar quais dos 12 requisitos essenciais para uma Política de Segurança da Informação, segundo a norma ABNT NBR ISO/IEC 27002:2013, estão presentes nas referidas Políticas.

Durante o mapeamento registrou-se “NÃO” para os itens que não constam nas políticas de segurança da informação. Para os itens que constam nas PSIC registrou-se a localização da informação no documento.

### 4.1.1 PSIC do Supremo Tribunal Federal

Por meio da Resolução nº 396, publicada em 23 de abril de 2009, o Supremo Tribunal Federal instituiu a sua Política de Segurança da Informação e Comunicação, a tabela 2 apresenta quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

**Tabela 2 - Análise da PSIC do STF**

| Supremo Tribunal Federal | RESOLUÇÃO Nº 396, DE 23 DE ABRIL DE 2009 |
|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | NÃO |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | NÃO |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | Texto Inicial e Artigo 2º |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | Artigo 1º |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | NÃO |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | Artigos 3º a 8º |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | NÃO |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | Artigo 14º |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | NÃO |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | NÃO |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | NÃO |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | NÃO |

### 4.1.2 PSIC do Supremo Tribunal de Justiça

O Supremo Tribunal de Justiça não possui uma Resolução ou Portaria específica que instituísse a sua Política de Segurança da Informação. Existem diversas Resoluções e Portarias que tratam de assuntos específicos e que no seu conjunto poderiam fazer parte da PSIC deste tribunal superior. Além desses normativos, o STJ elaborou uma cartilha de segurança da informação que trata do tema em questão e referencia as resoluções e portarias citadas anteriormente.

Neste trabalho, será considerado como Política de Segurança da Informação do STJ, o conjunto de resoluções e portarias referenciados na cartilha de segurança da informação elaborada pelo tribunal, bem como a própria cartilha que complementa as informações contidas nos normativos.

Após análise de cada normativo referenciado, será incluída uma nova coluna que terá por objetivo consolidar as análises realizadas.

A tabela 3 apresenta quais requisitos, segundo a ISO 27002:2013, estão previstos nestes documentos.

**Tabela 3 - Análise da PSIC do STJ**

| Superior Tribunal de Justiça | PORTARIA N. 25, DE 1 DE FEVEREIRO DE 2008 | PORTARIA STJ N. 445 DE 13 DE NOVEMBRO DE 2012 | RESOLUÇÃO N. 20 DE 9 DE AGOSTO DE 2012 | RESOLUÇÃO N. 8, DE 13 DE NOVEMBRO DE 2009 | CARTILHA SEGURANÇA DA INFORMAÇÃO 09/06/2014 | CONSOLIDADO |
|---|---|---|---|---|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | Não | Não | Não | Não | Página 14 | Sim |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | Não | Não | Não | Não | Não | Não |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | Não | Não | Não | Não | Página 5 | Sim |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | Não | Não | Não | Não | Página 5 | Sim |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | Não | Não | Não | Não | Algumas páginas 12 | Sim |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | Não | Não | Não | Não | Página 11 | Sim |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | Não | Não | Não | Não | Não | Não |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | Artigo 6º | Não | Não | Não | Não | Sim |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | Não | Sim | Não | Não | Não | Sim |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | Não | Não | Não | Não | SIM | Sim |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | Não | Não | Não | Não | Não | Não |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | Não | Não | Não | Não | Não | Não |

### 4.1.3 PSIC do Superior Tribunal Militar

O Superior Tribunal Militar, por meio de sua ouvidoria, respondeu a solicitação de apresentação de sua política de segurança da informação com a mensagem abaixo:

"*Vossa Senhoria encaminhou uma mensagem à Ouvidoria do Superior Tribunal Militar (STM), órgão da Justiça Militar da União, o mais antigo tribunal superior do País criado em 1º de abril de 1808, que passou a integrar o Poder Judiciário a partir da Constituição de 1934, atuando, ininterruptamente, há mais de duzentos anos.*

*A Justiça Militar da União é a Justiça Especializada na aplicação da lei a uma categoria especial, a dos militares federais: Marinha, Exército e Aeronáutica e, em certos casos, os civis, julgando apenas e tão somente os crimes militares definidos em lei.*

*Em atenção a manifestação de Vossa Senhoria, após consulta ao Comitê Gestor de Segurança da Informação da Justiça Militar da União, informamos o seguinte:*

*"- Consoante o que prescreve a Resolução nº 194, de 28 de agosto de 2013, compete ao Ministro Vice-Presidente do Superior Tribunal Militar presidir o Comitê Gestor de Segurança da Informação da Justiça Militar da União, implementando a série de medidas prescritas na Resolução nº 90/2009 do Conselho Nacional de Justiça;*

*- Nessas condições, após assumir a Vice-Presidência do STM, o Ministro ARTUR VIDIGAL DE OLIVEIRA convocou reunião do Comitê Gestor de Segurança da Informação, reunião esta que foi realizada no dia 18 de maio último, ocasião em que empossou um Grupo de Trabalho que, no prazo máximo de 90 (noventa) dias, submeterá ao Comitê Gestor proposta de Política de Segurança da Informação da Justiça Militar da União. Portanto, espera-se que até 17 de agosto de 2015, esteja o Comitê Gestor apreciando a Política de Segurança da Informação, para posterior submissão ao Plenário do STM;*

*- Após a aprovação da Política de Segurança da Informação, pretende o Comitê Gestor acelerar a elaboração dos Planos decorrentes, sejam eles*

*estratégicos, táticos ou operacionais, de forma a, até o final do corrente ano, possuir a Justiça Militar da União todo o planejamento necessário da Segurança da Informação, iniciando a implementação de medidas e práticas necessárias à proteção física do pessoal e das instalações, bem como a proteção da informação nos seus diversos segmentos".*

Diante da resposta encaminhada pela Ouvidoria do Superior Tribunal Militar, para efeitos de análise, vamos considerar que a política de segurança da informação do Superior Tribunal Militar é inexistente e, portanto, não contempla os requisitos essenciais para uma política de segurança da informação, segundo a norma NBR ISO/IEC 27002:2013.

### 4.1.4 PSIC do Tribunal Superior Eleitoral

Por meio da Resolução nº 22.780, publicada em 24 de abril de 2008, o Tribunal Superior Eleitoral instituiu a sua Política de Segurança da Informação e Comunicação, a tabela 4 apresenta quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

**Tabela 4 - Análise da PSIC do TSE**

| **Tribunal Superior Eleitoral** | **RESOLUÇÃO Nº 22.780, DE 24 DE ABRIL DE 2008** |
|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | NÃO |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | CAPÍTULO II |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | CAPÍTULOS I e III |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | CAPÍTULO II |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | NÃO |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | CAPÍTULO VIII |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | ARTIGO 20 |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | NÃO |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | CAPÍTULO VI |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | NÃO |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | NÃO |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | ARTIGO 21 |

### 4.1.5 PSIC do Tribunal Superior do Trabalho

Por meio do Ato nº 764/GDGSET.GP, publicada em 27 de novembro de 2012, o Tribunal Superior do Trabalho instituiu a sua Política de Segurança da Informação e Comunicação, a tabela 5 apresenta quais requisitos, segundo a ISO 27002:2013, estão previstos neste documento.

**Tabela 5 - Análise da PSIC do TST**

| **Tribunal Superior do Trabalho** | **ATO Nº 764/GDGSET.GP, DE 27 DE NOVEMBRO DE 2012** |
|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | CONSIDERAÇÕES INICIAIS |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | NÃO |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | ARTIGO 2 |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | NÃO |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | NÃO |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | NÃO |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | ARTIGO 78 |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | NÃO |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | CAPÍTULOS DE I A IX |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | NÃO |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | ARTIGO 81 |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | NÃO |

## 4.2 Consolidação dos requisitos identificados nas PSIC dos Tribunais

A tabela 6 apresenta, de forma consolidada, quais os requisitos necessários para uma PSIC, segundo a ISO 27002:2013, estão contempladas nas Políticas de Segurança da Informação de cada Tribunal Superior.

**Tabela 6 - Análise Consolidada das PSIC dos Tribunais Superiores**

| Requisitos necessários para uma PSIC segundo a ISO 27002:2013 | Supremo Tribunal Federal | Superior Tribunal de Justiça | Superior Tribunal Militar | Tribunal Superior do Trabalho | Tribunal Superior Eleitoral |
|---|---|---|---|---|---|
| 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | NÃO | SIM | NÃO | SIM | NÃO |
| 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | NÃO | NÃO | NÃO | NÃO | SIM |
| 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | SIM | SIM | NÃO | SIM | SIM |
| 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | SIM | SIM | NÃO | NÃO | SIM |
| 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | NÃO | SIM | NÃO | NÃO | NÃO |
| 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | SIM | SIM | NÃO | NÃO | SIM |
| 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | NÃO | NÃO | NÃO | SIM | SIM |
| 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | SIM | SIM | NÃO | NÃO | NÃO |
| 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | NÃO | SIM | NÃO | SIM | SIM |
| 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | NÃO | SIM | NÃO | NÃO | NÃO |
| 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | NÃO | NÃO | NÃO | SIM | NÃO |
| 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | NÃO | NÃO | NÃO | NÃO | SIM |

## 4.3 Análise do mapeamento dos requisitos

### 4.3.1 Quantidade de requisitos por grupo de atributos

Seguindo a metodologia aplicada por Ferrer e Lyra (2014), os 12 requisitos essenciais foram categorizados em 3 grandes grupos por apresentarem atributos semelhantes.

Conforme apresentado na tabela 7, o primeiro grupo de atributos foi chamado de Regulação e abrange 4 dos 12 requisitos essenciais. O segundo grupo foi denominado como Prevenção e/ou Controle abarcando 5 dos 12 requisitos. O terceiro grupo de atributos recebeu o nome de Responsabilidades e/ou Penalidades e agrupa 3 dos 12 requisitos.

Na tabela 7, foi contabilizado, em porcentagem, para cada um dos requisitos, a sua presença nas PSIC dos tribunais mapeados. Em seguida, foi feito o cálculo do percentual médio dos requisitos atendidos separado por cada um dos grandes grupos.

Baseado no percentual médio apresentado na tabela 7, é possível ranquear os três grandes grupos e identificar qual grupo de atributo tem maior e menor relevância na análise conjunta das PSIC dos tribunais.

Observa-se que 50% dos tribunais mapeados possuem atributos do tipo Regulação em suas PSIC, 40% dos tribunais mapeados contemplam atributos relacionados à Responsabilidade e/ou Penalidades e por fim, 32% dos tribunais mapeados têm presentes em suas PSIC atributos relacionados a Prevenção e/ou controles.

No grupo de atributos Regulação, o requisito *3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação?* esteve presente em todas PSIC. Portanto, constata-se a presença de uma importante característica nas PSIC analisadas, a clareza. Uma Política precisa ser de fácil compreensão por quem precisar conhecê-la e cumpri-la. O requisito *5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação?* foi o item que menos esteve presente nas PSIC dos tribunais o que indica a necessidade dos tribunais buscarem deixar mais claro ao seus colaboradores o que

se pretende alcançar quando se estabelece políticas a serem cumpridas. Sem uma razão de ser, uma regra tem grandes chances de não ser cumprida.

Para o grupo de atributos Responsabilidades e/ou Penalidades, o requisito “6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? ” apesar de ter sido encontrado com maior frequência nas PSIC dos tribunais, é um item que merece atenção no sentido de se aperfeiçoar e deixar melhor definido cada um dos papéis e suas responsabilidades. Em nenhuma das PSIC em que esse requisito foi identificado, o requisito é atendido em sua plenitude. Já o requisito menos identificado nas PSIC, dentro do referido grupo de atributos, é o “12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? ”. Esse requisito poderia ser facilmente integrado às PSIC, assim como fez o TSE, e garantir um alto impacto em sua credibilidade quando fica explícito para os colaboradores o apoio da direção. Essa ausência pode se justificar por se tratarem de resoluções e portarias, ou seja, normativos que precisam ser seguidos obrigatoriamente pelos servidores dos tribunais

Por fim, dentro do grupo de atributos Prevenção e/ou Controles, o requisito “9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? ” se destacou entre os requisitos que mais foram identificadas em todas as PSIC de todas as categorias. Esse fato se justifica, pois, esse requisito trata de assuntos mais práticos da política o que acaba sendo mais fácil de ser lembrado no momento da elaboração de um documento para essa finalidade. Já o requisito “11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) ” foi um dos menos identificados nas PSIC. A única PSIC que possuía artigo atribuindo a responsabilidade de revisão anual da PSIC, não teve essa ação concretizada. Este fato pode ser comprovado até mesmo pelas datas de publicação das políticas, datadas entre 2008 e 2012 e vigentes até o momento da solicitação das PSIC via Lei de Acesso à informação, em 2015.

**Tabela 7 - Categorização dos Requisitos Essenciais**

| Atributo dos Requisitos | Requisitos necessários para uma PSIC segundo a ISO 27002:2013 | % dos requisitos atendidos pelos órgãos analisados | % Médio dos requisitos verificados por atributo |
|---|---|---|---|
| Regulação | 1 - Contém a regulamentação, legislação e contratos que a PSIC deve estar amparada? | 40,00% | 50,00% |
| | 3 - Há o escopo, conceitos, definições e a descrição da importância da Segurança da Informação? | 80,00% | |
| | 4 - Os Princípios da Política de Segurança da Informação e Comunicação estão declarados? | 60,00% | |
| | 5 - Há objetivos e princípios para orientar todas as atividades relativas à segurança da informação? | 20,00% | |
| Prevenção e/ou Controles | 2 - Contém uma estrutura para estabelecer os objetivos de controle e os controles; a estrutura de análise; a avaliação e o gerenciamento de controle e a avaliação e o gerenciamento de risco? | 20,00% | 32,00% |
| | 7 - Há previsão para o processo de gestão de continuidade do negócio na PSIC? (Gestão da Continuidade de Negócios) | 40,00% | |
| | 9 - Há políticas específicas que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos (ex.: controle de acesso; classificação e tratamento da informação, etc.)? | 60,00% | |
| | 10 - As políticas de segurança da informação e comunicação são comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação? | 20,00% | |
| | 11 - As políticas de segurança da informação e comunicação são analisadas criticamente em intervalos planejados? (Atualização) | 20,00% | |
| Responsabilidades e/ou Penalidades | 6 - Há a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos? | 60,00% | 40,00% |
| | 8 - Caso haja violação da PSIC, há declaração das consequências neste documento? (Penalidades) | 40,00% | |
| | 12 - Há a declaração do comprometimento da Direção apoiando as metas e princípios da organização? | 20,00% | |

### 4.3.2 Quantidade de requisitos por cada tribunal

Na tabela 08, observa-se a quantidade de requisitos presentes em cada uma das políticas se segurança da informação e comunicação conforme a ISO NBR 27002:2013, em cada um dos tribunais superiores.

**Tabela 8 - Quantidade de requisitos atendidos nos órgãos analisados**

| Tribunal | Quantidade de requisitos verificados | % requisitos verificados no órgão |
|---|---|---|
| Supremo Tribunal Federal | 4 | 33,33% |
| Superior Tribunal de Justiça | 8 | 66,67% |
| Superior Tribunal Militar | 0 | 0,00% |
| Tribunal Superior Eleitoral | 7 | 58,33% |
| Tribunal Superior do Trabalho | 5 | 41,67% |

Para aplicação da metodologia que estabelecerá o nível de maturidade das PSIC onde se aplica a média aritmética e Desvio-Padrão, vamos desconsiderar o STM. Ele será incluído nas análises posteriormente.

Constata-se que nas políticas de segurança da informação dos tribunais superiores, a média de requisitos presentes é de 6 ou 50% de requisitos identificados. Dos quatro tribunais analisados, dois estão acima da média (STJ e TSE) e dois ficaram abaixo (TST e STF).

## 4.4 Nível de Maturidade

Baseado na metodologia estabelecida por Ferrer e Lyra (2014), a média aritmética dos requisitos identificados nas PSIC é de 6. O cálculo do desvio-padrão destes requisitos é de 1,58. Portanto, para considerar uma PSIC com grau de maturidade alto, o número de requisitos identificados deve estar acima do valor do somatório da média com o desvio padrão, nesse caso, 7,58. O grau de maturidade definido como bom, o número de requisitos deve estar entre a média aritmética e o somatório entre a média aritmética e o desvio-padrão. Para o presente estudo, o resultado seria entre 6 e 7,58. Para atingir o grau de maturidade razoável, o número de requisitos deve variar entre o valor do desvio-padrão e a média aritmética, ou

seja, entre 1,58 e 6. Por fim, o grau de maturidade ruim é atribuído às políticas de segurança cujo número de requisitos identificados não superam o valor de desvio-padrão.

Os resultados destes cálculos estão representados na tabela 09, onde é apresentado o grau de maturidade de cada uma das Políticas de Segurança dos tribunais superiores.

**Tabela 9 - Matriz de maturidade das Políticas de Segurança da Informação**

| Média da quantidade de requisitos verificados nas PSIC analisadas | Grau de Maturidade | Quantidade de órgãos analisados que atendem a esta faixa de requisitos |
|---|---|---|
| Acima de 7,58 | alto | 1 (STJ) |
| Entre 6 e 7,58 | bom | 1 (TSE) |
| Entre 1,78 e 6 | razoável | 2 (TST e STF) |
| Menor que 1,78 | a desejar | 1 (STM) |

O Superior Tribunal de Justiça foi o tribunal superior que atingiu o grau de maturidade alto, seguido pelo Tribunal Superior Eleitoral que obteve grau de nível bom. O Tribunal Superior do Trabalho e o Supremo Tribunal Federal angariaram o grau de maturidade razoável e por fim, o Superior Tribunal Militar obteve grau de maturidade a desejar.

## 4.5 Análise comparativa do Nível de Maturidade entre Poder Executivo e Judiciário

Ferrer (2014) apresenta a tabela 10 que evidencia o nível de maturidade das Políticas de Segurança da Informação do Poder Executivo. Observa-se que o grau de maturidade identificado nos tribunais superiores do judiciário brasileiro é inferior ao mapeado nos órgãos do Executivo.

**Tabela 10 - Matriz de maturidade das PSIC (Poder Executivo)**

| Média da quantidade de requisitos verificados nas PSIC analisadas | Grau de Maturidade | Quantidade de órgãos analisados que atendem a esta faixa de requisitos |
|---|---|---|
| Acima de 10,97 | alto | 4 |
| Entre 8,9 e 10,97 | bom | 2 |
| Entre 6,83 e 8,9 | razoável | 3 |
| Menor que 6,83 | a desejar | 1 |

Esse fato é reforçado ao comparar a média da quantidade de requisitos verificados nas PSIC do Judiciário e do Executivo. Observando as tabelas 9 e 10, percebe-se que a média relacionada ao grau de maturidade “alto” no poder Judiciário, equivale a um grau de maturidade “razoável” no poder executivo.

Mais uma evidência que corrobora para análise comparativa entre os poderes está na análise das tabelas 8 e 11. O órgão do poder executivo, que menos requisitos foram identificados, em sua PSIC, apresenta seis dos doze requisitos. Já no Poder Judiciário, o tribunal superior que mais requisitos estavam presentes, verificou-se oito requisitos.

**Tabela 11 - Quantidade de requisitos atendidos (Poder Executivo)**

| Órgão | Quantidade de requisitos verificados | % requisitos verificados no órgão |
|---|---|---|
| Ministério do Turismo | 12 | 100,00% |
| Ministério da Ciência e Tecnologia e Inovação | 11 | 91,67% |
| MPOG/ Secretaria do Orçamento Federal | 11 | 91,67% |
| Ministério da Defesa | 11 | 91,67% |
| Ministério da Justiça | 9 | 75,00% |
| Ministério da Cultura | 8 | 66,67% |
| Ministério do Trabalho e Emprego | 7 | 58,33% |
| Ministério da Educação | 7 | 58,33% |
| Ministério da Agricultura | 7 | 58,33% |
| Ministério da Saúde | 6 | 50,00% |

Em relação ao grupo de atributos, a análise do Poder Executivo identifica uma maior preocupação nas PSIC com Prevenção e/ou Controle, seguido pela Regulação e por fim Responsabilidades e/ou Penalidades. Já no Poder Judiciário, a maior preocupação nas Políticas refere-se à Regulação, seguido pelas Responsabilidades e/ou Penalidades e por fim Prevenção e/ou Controles.

# CONCLUSÃO

Este estudo verificou o nível de maturidade das Políticas de Segurança da Informação dos tribunais superiores do judiciário brasileiro, identificando sua aderência às melhores práticas e realizando a análise de maturidade, baseado na metodologia desenvolvida e aplicada por Ferrer e Lyra (2014) para os órgãos do Poder Executivo.

Foi objeto deste trabalho, também, realizar uma análise comparativa entre os níveis de maturidade observados por Ferrer e Lyra (2014) para os órgãos do Poder Executivo, e os resultados observados neste trabalho para o Poder Judiciário.

Constatou-se que os órgãos do Poder Executivo contemplam em suas políticas de segurança da informação um maior número de requisitos elencados como essenciais à uma PSIC em comparação aos órgãos do Poder Judiciário.

Este fato se concretiza ao quando se compara os números obtidos entre o estudo sobre o Poder Executivo e Poder Judiciário no que tange ao nível de maturidade e verifica-se que o nível de maturidade alto para uma política de segurança da informação do Poder Judiciário refere-se a uma política de maturidade razoável para o Poder Executivo.

Entre os tribunais superiores, o Superior Tribunal de Justiça apresentou o maior nível de maturidade em sua política de segurança da informação e o Superior Tribunal Militar apresentou o menor nível de maturidade, já que à época o STM não possuía uma política de segurança da informação vigente.

Este estudo permitiu, também, perceber que as Políticas de Segurança dos tribunais superiores têm uma positiva preocupação em serem de fácil entendimento, porém deixam a desejar em suas justificativas sobre a razão de determinadas regras estarem contempladas em suas Políticas.

Considerando que o decreto que determina a instituição de políticas de segurança da informação em órgãos dos três poderes ser datado do ano 2000, o resultado obtido por esse estudo nos permite concluir que este assunto carece de muita atenção e uma série de ações para se atingir um nível aceitável para órgãos

com tamanha responsabilidade e importância, como os tribunais superiores, instâncias máximas do Poder Judiciário Brasileiro.

Um primeiro passo na busca pela elevação do nível de maturidade das políticas, como sugestão, poderia ser a disseminação para os comitês de segurança da informação de cada órgão, a adoção dos requisitos indispensáveis para uma PSIC, elaborado por Ferrer e Lyra (2014) como direcionadores na elaboração das próximas versões de suas PSIC.

A análise dos tribunais superiores não traduz inteiramente o cenário da segurança da informação do judiciário brasileiro. Esse trabalho pode servir de ponto de partida para uma análise mais detalhada sobre os demais tribunais de outras instâncias, buscando uma melhor percepção de como o judiciário brasileiro está aderente ao que determina o decreto nº 3.505, de 13 de junho de 2000.

Além do mais, a análise realizada por este estudo é meramente quantitativa e não qualitativa. Esse tipo de análise não leva em conta possíveis ações que possam ser executadas por cada órgão e que visem garantir a aplicação de alguns dos requisitos essenciais para uma PSIC mesmo não registradas formalmente pelo instrumento objeto deste estudo, ou seja, a Política de Segurança da Informação.

Como os valores obtidos no presente estudo divergem dos valores obtidos por Ferrer e Lyra (2014), observa-se que a metodologia abre o precedente para que uma política de segurança considerada nível de maturidade alto também possa ser classificada como maturidade razoável, a depender do grupo de políticas em análise. Sugere-se aprimorar a metodologia adotando valores fixos à matriz de maturidade a fim de se obter uma análise sob uma mesma perspectiva sobre todas as políticas analisadas pela referida metodologia.

Por fim, é gratificante perceber que o presente trabalho pôde contribuir com a melhoria do nível de maturidade da política de segurança da informação de pelo menos um dos tribunais já que até o início desse trabalho não havia um comitê de segurança da informação nomeado e o levantamento de dados para embasar essa análise foi o gatilho para que o trabalho de elaboração da política de segurança fosse iniciado neste órgão.

# REFERÊNCIAS


ABNT. Tecnologia da informação - Técnicas de segurança - **Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013

BEAL, A. **Segurança da Informação**: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. 1ed. São Paulo: Atlas, 2008

BRASIL. **Decreto nº. 3.505, de 13 de junho de 2000**: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 06 set. 2015.

Controladoria Geral da União. **LAI: A Lei de Acesso à Informação**. Disponível em: <http://www.acessoainformacao.gov.br/assuntos/conheca-seu-direito/a-lei-de-acesso-a-informacao>. Acesso em: 10 nov. 2015

DANTAS, M. **Segurança da Informação**: uma abordagem focada em gestão de riscos. 1ed. Olinda: Livro Rápido, 2011.

FERNANDES, A.; ABREU, V. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. 3ed. Rio de Janeiro: Brasport, 2012.

FERREIRA, F.N.F. **Segurança da Informação**. 1ed. Rio de Janeiro, Ciência Moderna, 2003

FERREIRA, F.N.F.; ARAÚJO, M.T. **Política de Segurança da Informação**: Guia Prático para Elaboração e Implementação. 1ed. Rio de Janeiro: Ciência Moderna, 2006.

FERRER, J.C.S.; LYRA, M. **Análise da Maturidade da Política de Segurança da Informação dos Órgãos da Administração Pública Federal Direta,** Brasília, 2014. Monografia de Pós-graduação em Governança em Tecnologia da Informação. Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília.

FONTES, E.L.G. **Políticas e Normas para a Segurança da Informação**: como desenvolver e manter regulamentos para a proteção da informação nas organizações. 1ed. Rio de Janeiro, Brasport, 2012.

FONTES, E.L.G. **Praticando a segurança da informação**. 1ed. Rio de Janeiro, Brasport, 2008.

IBGC - Instituto Brasileiro de Governança Corporativa. **Princípios Básicos da Governança Corporativa.** Disponível em: <http://www.ibgc.org.br/inter.php?id=18163>. Acesso em: 01 set. 2015

LYRA, M.R. **Segurança e Auditoria em sistemas de informação**. 1ed. Rio de Janeiro, Ciência Moderna, 2008.

MANOEL, S.S. **Governança de Segurança da Informação**: Como criar oportunidades para o seu negócio. 1ed. Rio de Janeiro, Brasport, 2014.

SÊMOLA, M. **Gestão da Segurança da Informação** – Uma visão executiva. 3ed. Rio de Janeiro: Elsevier, 2003.

Superior Tribunal de Justiça. **Cartilha de Segurança da Informação.** Brasília, 2014. Conscientizar cada servidor do seu papel dentro da Segurança da Informação. Ângela Merce Teixeira Neves. Brasília – DF.

Superior Tribunal de Justiça. **Portaria nº 25 de 1 de Fevereiro de 2008**.Brasília, 2008. Estabelece diretrizes para a segurança da informação do Supremo Tribunal Federal e dá outras providências. Gilmar Mendes. Brasília – DF.

Superior Tribunal de Justiça. **Portaria STJ nº 445 de 13 de Novembro de 2012**.Brasília, 2012. Dispõe sobre o uso do serviço de correio eletrônico e sobre a administração do respectivo software no Superior Tribunal de Justiça. Felix Fischer. Brasília – DF.

Superior Tribunal de Justiça. **Resolução nº 20 de 9 de Agosto de 2012**.Brasília, 2012. Dispõe sobre a certificação digital no Superior Tribunal de Justiça e dá outras providências. Ari Pargendler. Brasília – DF.

Superior Tribunal de Justiça. **Resolução nº 8 de 13 de Novembro de 2009**. Brasília, 2009. Institui o Código de Conduta do Superior Tribunal de Justiça. Cesar Asfor Rocha. Brasília – DF.

Supremo Tribunal Federal. **Resolução nº 396 de 23 de Abril de 2009**.Brasília, 2009. Estabelece diretrizes para a segurança da informação do Supremo Tribunal Federal e dá outras providências. Gilmar Mendes. Brasília – DF.

## ANEXO A: PSIC do Supremo Tribunal Federal

## RESOLUÇÃO Nº 396, DE 23 DE ABRIL DE 2009

Estabelece diretrizes para a segurança da informação do Supremo Tribunal Federal e dá outras providências.

**O PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL**, nos termos do artigo 361, inciso I, do Regimento Interno, tendo em vista o contido no Processo nº 331.217/2008,

considerando que o Tribunal, no exercício de suas competências, gera, adquire e absorve informações, que devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

considerando que as informações no Tribunal são armazenadas em diferentes meios, veiculadas por diferentes formas e, portanto, vulneráveis a incidentes em segurança da informação;

considerando que a adequada gestão da informação precisa nortear todos os processos de trabalho e deve ser impulsionada por política corporativa de segurança da informação;

RESOLVE:

Art. 1º A atividade de segurança da informação no Supremo Tribunal Federal abrange aspectos físicos, tecnológicos e humanos e orienta-se pelos seguintes princípios:

I - confidencialidade: garante que a informação seja acessada somente pelas pessoas que tenham autorização para tal;

II - disponibilidade: garante que as informações estejam acessíveis às pessoas autorizadas, no momento requerido;

III - integridade: garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.

Art. 2º Para os efeitos desta Resolução, ficam estabelecidas as seguintes conceituações:

I - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

II - segurança da informação: proteção da informação contra ameaças para garantir a continuidade das atividades do Tribunal e minimizar os riscos;

III - gestor da informação: servidor, unidade ou estrutura *ad hoc* que, no exercício de suas competências, seja responsável pela produção de informações, pela definição de requisitos de soluções de tecnologia da informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues ao Tribunal;

IV - custodiante: servidor, unidade ou estrutura *ad hoc* que detenha a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal;

V - incidente em segurança da informação: fraude, sabotagem, desvio, falha de equipamentos, acessos não autorizados, mau uso, extravio, furto ou evento indesejado ou inesperado que possa comprometer as atividades do Tribunal ou ameaçar a segurança da informação;

VI - usuário interno: qualquer servidor, ocupante de posto de trabalho, prestador de serviço terceirizado, estagiário ou qualquer outro colaborador que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo STF;

VII - usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não seja caracterizada como usuário interno.

Art. 3º Os usuários internos e externos que, de forma autorizada, tenham acesso a informações produzidas ou custodiadas pelo STF estão sujeitos às disposições sobre segurança da informação constantes desta Resolução e demais normativos.

Art. 4º Compete ao Comitê Gestor de Segurança da Informação do Supremo Tribunal Federal gerir a segurança das informações do STF, bem como:

I - elaborar e submeter à Secretaria do Tribunal estudos sobre planejamento, controle, políticas e ações de segurança da informação;

II - apresentar à Secretaria do Tribunal os resultados da segurança da informação;

III - definir critérios, gerenciar e avaliar os resultados de auditorias de conformidade de segurança da informação e de aspectos legais relacionados à proteção das informações do STF;

IV - definir critérios e parâmetros de avaliação de conformidade da gestão e execução de serviços de segurança da informação;

V - coordenar e acompanhar a implementação de ações sobre segurança da informação;

VI - monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal;

VII - apoiar as unidades do Tribunal na adoção de medidas que garantam a continuidade das suas atividades e o retorno à situação de normalidade em caso de incidente em segurança da informação;

VIII - coordenar ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de segurança da informação, com apoio das demais unidades do Tribunal.

Parágrafo único. Cabe às unidades do Tribunal implementar e acompanhar ações de segurança da informação nas respectivas áreas de atuação.

Art. 5º Compete ao gestor da informação:

I - definir critérios de classificação e procedimentos de acesso às informações, observados os dispositivos legais e normas internas referentes ao sigilo e a outros requisitos de classificação;

II - propor regras específicas para o uso das informações.

Art. 6º Compete ao custodiante da informação:

I - zelar pela segurança da informação sob sua custódia, conforme os critérios definidos pelo respectivo gestor da informação;

II - comunicar tempestivamente ao gestor situações que comprometam a segurança das informações sob sua custódia;

III - comunicar ao gestor eventuais limitações ao cumprimento dos critérios definidos para segurança da informação.

Art. 7º Compete aos titulares das unidades do Tribunal, no que se refere à segurança da informação:

I - colaborar na conscientização dos usuários internos sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade práticas inerentes à segurança da informação;

III - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários internos sob sua supervisão.

Art. 8º Compete aos usuários internos garantir a segurança das informações a que tenham acesso e comunicar ao Comitê Gestor de Segurança da Informação os incidentes de que tenham conhecimento.

Art. 9º O acesso às informações produzidas ou custodiadas pelo Tribunal, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários.

Parágrafo único. Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários necessitará de prévia autorização formal do gestor da informação.

Art. 10. As medidas de segurança da informação devem ser planejadas, aplicadas, implementadas e, periodicamente, reavaliadas de acordo com os objetivos institucionais e os riscos para as atividades do STF.

Art. 11. A classificação das informações produzidas ou custodiadas pelo Tribunal deve indicar a necessidade, a prioridade e o grau de proteção dessas

informações, durante todo o seu ciclo de vida, com níveis e critérios para sua criação, manuseio, transporte, armazenamento e descarte.

Art. 12. As informações produzidas por usuários internos, no exercício de suas funções, são patrimônio intelectual do STF e não cabe a seus criadores qualquer forma de direito autoral.

Parágrafo único. Quando as informações forem produzidas por terceiros para uso exclusivo do Tribunal, a obrigatoriedade do seu sigilo deve ser estabelecida em instrumento adequado.

Art. 13. As normas editadas pelo Tribunal, relacionadas à segurança da informação, deverão observar as disposições estabelecidas nesta Resolução.

Art. 14. A inobservância dos dispositivos desta Resolução pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 15. Fica revogado o art. 2º da Resolução nº 371, de 18 de julho de 2008.

Art. 16. Esta Resolução entra em vigor na data de sua publicação.

## ANEXO B: PSIC do Superior Tribunal de Justiça

### PORTARIA N. 25, DE 1 DE FEVEREIRO DE 2008.

Institui a política de utilização dos recursos de tecnologia da informação no âmbito do Superior Tribunal de Justiça.

**O PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA,** usando da atribuição que lhe é conferida pelo art. 21, XXXI, do Regimento Interno,

**RESOLVE:**

Art. 1º Os recursos de informática disponibilizados nas diversas áreas do Tribunal destinam-se, exclusivamente, ao atendimento das necessidades do serviço.

§ 1º Os arquivos gerados no ambiente computacional do STJ são de propriedade exclusiva do Tribunal.

§ 2º É proibida a utilização dos recursos de informática disponibilizados pelo Tribunal para acesso, guarda e divulgação de material incompatível com ambiente do serviço e que viole direitos autorais ou que venha infringir a legislação vigente.

§ 3º É proibida a instalação de recursos de informática que não tenham sido homologados e/ou adquiridos pela área de Tecnologia da Informação.

Art. 2º É responsabilidade da área de Tecnologia da Informação prover e controlar o uso dos recursos de informática, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional.

Art. 3º O acesso aos recursos de informática é concedido mediante solicitação de titular de unidade à área de Tecnologia da Informação.

§ 1º Aos usuários são fornecidos mecanismos de identificação, autenticação e autorização baseados em conta e senha e/ou certificação digital, de uso pessoal e intransferível, vedada sua divulgação a terceiros.

§ 2º O uso indevido destes mecanismos responsabiliza tanto quem permitiu ou facilitou o acesso, quanto quem os utilizou.

§ 3º É responsabilidade do titular da unidade solicitar a alteração nas permissões de uso, quando de movimentação, afastamento, desligamento ou em situação de infração desta norma.

Art. 4° Todas as operações realizadas com uso dos recursos de informática serão registradas para fins de auditoria.

Art. 5º Cabe à área de Tecnologia da Informação editar normas técnicas e procedimentais.

Art. 6º O descumprimento destas normas ensejará apuração de responsabilidade mediante processo disciplinar.

Art. 7º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço, ficando revogado o Ato 138 de 13/11/2001.

**PORTARIA STJ N. 445 DE 13 DE NOVEMBRO DE 2012.**

Dispõe sobre o uso do serviço de correio eletrônico e sobre a administração do respectivo software no Superior Tribunal de Justiça.

O **PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA**, usando da atribuição conferida pelo inciso XXXI do art. 21 do Regimento Interno e considerando o que dispõem a Resolução CNJ n. 45, de 17 de dezembro de 2007, a Portaria STJ n. 25 de 1º de fevereiro de 2008 e a Resolução STJ n. 8 de 13 de novembro de 2009, sobretudo os arts. 7º e 11, bem como o que consta do processo administrativo STJ n. 12.162/2010 e da Nota Técnica da Assessoria Jurídica da Secretaria do Tribunal juntada aos mencionados autos,

**RESOLVE:**

## CAPÍTULO I

## Da Finalidade

Art. 1º Esta portaria disciplina o uso do serviço de correio eletrônico no Superior Tribunal de Justiça e estabelece regras quanto à administração do software dessa ferramenta.

Art. 2º O serviço de correio eletrônico é instrumento de caráter institucional que visa à comunicação entre seus usuários e entre estes e o público externo, de forma ágil e eficiente.

## CAPÍTULO II

## Das Definições

Art. 3º Para os efeitos desta portaria, consideram-se:

I – usuário: pessoa autorizada a acessar os sistemas e serviços disponíveis na rede de computadores do Superior Tribunal de Justiça, entre esses o serviço de correio eletrônico, por meio de uma conta de rede e senha;

II – usuário interno: ministros e quaisquer servidores ativos do Tribunal que tenham acesso, de forma autorizada, às informações produzidas ou custodiadas pelo órgão, devendo efetivamente exercer suas atividades no Tribunal;

Fonte: Boletim de Serviço [do] Superior Tribunal de Justiça, 13 nov. 2012.

III – usuário colaborador: prestador de serviço terceirizado, estagiário ou

qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, às

informações produzidas ou custodiadas pelo órgão;

IV – caixa postal: repositório de armazenamento de mensagens de correio

eletrônico integrante da base de dados dos equipamentos servidores de correio eletrônico

do órgão;

V – conta de rede: via de acesso identificado aos sistemas e serviços

computadorizados do Tribunal;

VI – endereço eletrônico: designação por meio da qual se identifica a caixa postal de uma unidade administrativa ou o usuário do serviço de correio eletrônico;

VII – serviço de correio eletrônico: sistema utilizado para criar, enviar, receber, ler, imprimir ou arquivar informações com o propósito de promover a comunicação entre os usuários, provendo a troca de mensagens entre usuários do Tribunal e desses com pessoas externas;

VIII – e-mail: conjunto de informações em formato digital encapsuladas em invólucro virtual em que consta, no mínimo, o endereço de correio eletrônico do destinatário;

IX – mensagem: informação criada, enviada, recebida, lida, impressa ou arquivada, com ou sem anexo, por meio do serviço de correio eletrônico;

X – mensagem armazenada: aquela aberta e mantida na caixa postal;

XI – anexo: qualquer arquivo de computador apensado à mensagem;

XII – lista de distribuição: agrupamento de diversos endereços eletrônicos em um único que, uma vez inserido como destinatário de uma mensagem, permite a distribuição desta a todas as caixas postais integrantes daquele;

XIII – armazenamento local: repositório de dados sob gestão direta do usuário, como arquivos de pastas particulares, no qual podem ser armazenados itens de correio eletrônico;

XIV – unidade administrativa: instância de gestão representada no organograma do Tribunal, conforme publicado em portaria;

XV – gestor de caixa postal: usuário responsável por caixa postal de uso individual ou coletivo ou de unidade administrativa.

Parágrafo único. A conta de rede de que trata o inciso V é pessoal, intransferível e de uso exclusivo da pessoa a quem foi atribuída, a qual é responsável por sua utilização.

## CAPÍTULO III

## Dos Usuários do Correio Eletrônico

Art. 4º Podem ser usuários do serviço de correio eletrônico do Tribunal:

I – ministro;

II – magistrado convocado;

III – servidor;

IV – terceirizado;

V – estagiário;

VI – colaborador eventual autorizado pelo Comitê Gestor do Serviço de Correio Eletrônico.

## CAPÍTULO IV

## Das Caixas Postais

Art. 5º As caixas postais classificam-se em:

I – caixa postal individual de usuário interno;

II – caixa postal individual de usuário colaborador;

III – caixa postal da unidade administrativa;

IV – caixa postal de uso coletivo.

Parágrafo único. A caixa postal de uso coletivo é destinada a grupo de

trabalho, comitê, comissão, projeto ou atividade específica de interesse do Tribunal.

Art. 6º As caixas postais são destinadas ao uso em serviço do Tribunal, devendo seus gestores zelar pelo bom uso do recurso, observado o disposto no inciso VI do art. 16.

Art. 7º As informações contidas nas caixas postais são consideradas institucionais, devendo, portanto, observar as normas de elaboração de atos administrativos previstas no Manual de Padronização de Textos do STJ.

Art. 8º As caixas postais individuais poderão ser utilizadas por mais de um usuário, desde que autorizado pelo seu gestor.

Art. 9º A Secretaria de Tecnologia da Informação e Comunicação realizará,

diária e semanalmente, cópia de segurança (backup) das mensagens das caixas de correio eletrônico e a manterá por períodos de 90 e 180 dias, respectivamente.

## CAPÍTULO V

## Das Responsabilidades e dos Papéis Exercidos

Art. 10. Cabe ao gestor de caixa postal:

I – examinar o conteúdo da caixa postal, dando tratamento adequado e tempestivo às mensagens recebidas, respeitadas as normas de segurança da informação;

II – adotar medidas para que o volume ocupado pelo conteúdo da caixa postal não exceda os limites estabelecidos;

III – conceder as permissões de acesso à caixa postal.

Parágrafo único. O gestor de caixa postal poderá delegar as ações previstas nos incisos I, II e III a outro usuário interno ou colaborador, mantida, contudo, a responsabilidade pelas ações praticadas.

## CAPÍTULO VI

## Do Comitê Gestor do Serviço de Correio Eletrônico

Art. 11. O Comitê Gestor do Serviço de Correio Eletrônico será composto por representantes das seguintes unidades do Tribunal:

I – Secretaria de Tecnologia da Informação e Comunicação;

II – Secretaria de Comunicação Social;

III – Secretaria do Tribunal.

Parágrafo único. O Comitê Gestor do Serviço de Correio Eletrônico será coordenado pelo titular da Secretaria de Tecnologia da Informação e Comunicação.

Art. 12. Compete ao Comitê Gestor do Serviço de Correio Eletrônico:

I – elaborar e divulgar regras de bom uso do serviço de correio eletrônico;

II – autorizar colaborador eventual a utilizar o serviço de correio eletrônico;

III – tomar as medidas previstas nos incisos I e II do caput do art. 17, bem como no § 2º;

IV – estabelecer limites operacionais para o sistema de correio eletrônico;

V – definir os termos do acesso remoto às caixas postais individuais;

VI – homologar o software a ser utilizado como cliente do sistema de correio eletrônico;

VII – verificar o tráfego, o conteúdo das mensagens transmitidas ou recebidas e os documentos e demais registros armazenados no sistema de correio eletrônico de propriedade do Superior Tribunal de Justiça nos termos do art. 24;

VIII – suspender o acesso a qualquer recurso do serviço de correio eletrônico, nos termos do § 3º do art. 24;

IX – acessar o conteúdo de caixas postais nos termos do art. 25;

X – estabelecer norma que trate da interface entre os sistemas corporativos e o correio eletrônico;

XI – criar, ativar, desativar e excluir caixa postal após o recebimento das solicitações relacionadas no CAPÍTULO XI.

Art. 13. Compete à Secretaria de Tecnologia da Informação e Comunicação definir a Equipe de Administradores do Correio Eletrônico.

Art. 14. Compete à Equipe de Administradores do Correio Eletrônico:

I – fazer a manutenção do sistema e a gerência das caixas postais;

II – homologar toda e qualquer solução de tecnologia de informação que se integre ao serviço de correio eletrônico para envio e recebimento automatizado de mensagens eletrônicas;

III – excluir as caixas postais que caiam em desuso;

IV – permitir a usuário colaborador o envio e recebimento de mensagens externas, nos termos do parágrafo único do art. 15.

## CAPÍTULO VII

## Dos Cuidados, das Restrições e das Penalidades

Art. 15. As caixas postais individuais de usuários colaboradores devem ser utilizadas exclusivamente para o envio e recepção de mensagens entre caixas postais do Tribunal.

Parágrafo único. O responsável pela unidade administrativa à qual o colaborador se encontrar subordinado poderá solicitar, por meio do SAC da Secretaria de Tecnologia da Informação e Comunicação, que seja facultado ao colaborador enviar e receber mensagens externas, quando o exigir a natureza de seu trabalho.

Art. 16. Devem ser observadas as seguintes diretrizes para uso do serviço de correio eletrônico:

I – são vedados o uso e a tentativa de acesso não autorizado às caixas postais de terceiros;

II – toda mensagem emitida por meio do serviço de correio eletrônico deve conter a identificação clara de seu remetente, vedado o anonimato e qualquer forma de descaracterização da autoria;

III – as mensagens devem ter conteúdo lícito, sendo vedados o envio e o armazenamento de mensagens que contenham:

a) matéria comercial, notadamente a oferta de produtos ou de serviços próprios ou de terceiros;

b) material obsceno, pornográfico ou antiético;

c) anúncios publicitários;

d) listas de endereços eletrônicos dos usuários do serviço de correio eletrônico;

e) vírus ou qualquer outro tipo de programa danoso aos sistemas de informática;

f) material que viole a lei de propriedade intelectual;

g) mensagens cuja fonte não possa ser confirmada, como entretenimentos, boatos e "correntes" eletrônicas;

h) material preconceituoso ou discriminatório;

i) assuntos ofensivos à moral e aos bons costumes;

j) músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

IV – é vedada a divulgação de endereços eletrônicos internos de terceiros sem a autorização do gestor da caixa para finalidades alheias às atividades do Tribunal;

V – é permitida ao usuário a utilização de seu endereço eletrônico em listas de discussão que tratem de assuntos relacionados exclusivamente ao interesse do trabalho, de conteúdo profissional ou educativo;

VI – é admitida a utilização do correio eletrônico institucional para fins pessoais, desde que sem prejuízo do serviço e atendidos os demais requisitos estabelecidos nesta portaria;

VII – o e-mail particular que inclui comunicação pessoal deve ser utilizado em conta pessoal via web, não sendo permitida a instalação de cliente (software) diferente daquele definido para o serviço de correio eletrônico do Tribunal;

VIII – é vedado o envio de mensagem em desacordo com o grau de confidencialidade atribuído a seu conteúdo;

IX – é vedado o envio ou armazenamento de mensagem de conteúdo ilegal ou em desacordo com o Código de Conduta do Superior Tribunal de Justiça, instituído pela Resolução n. 8 de 13 de novembro de 2009;

X – é vedado insistir no envio de mensagens a qualquer pessoa que não a deseje receber;

XI – é vedado deixar a estação desbloqueada com o cliente de correio eletrônico aberto e se ausentar da estação de trabalho;

XII – é vedado fornecer senha da conta de rede, de serviço de correio eletrônico ou de sistemas a outra pessoa ou fazer uso da senha de outra pessoa;

XIII – é vedado encaminhar ao serviço de correio eletrônico pessoal qualquer informação de uso exclusivo do Tribunal sem a devida autorização.

§ 1º Excetuam-se às restrições constantes do inciso III deste artigo os casos relacionados à apuração de infrações pelos órgãos competentes e à comunicação do fato à autoridade superior.

§ 2º Será considerada violação de sigilo funcional a divulgação do conteúdo de mensagem que tenha sido acessada em função de manutenção técnica ou restauração de cópias de segurança sem a autorização prévia do usuário.

Art. 17. A inobservância aos dispositivos desta portaria pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável:

I – advertência por escrito;

II – limitação temporária do uso do serviço de correio eletrônico do Tribunal;

III – outras sanções administrativas, civis e penais cabíveis.

§ 1º Na hipótese de reincidência ou diante da gravidade do fato, poderá ser caracterizada infração funcional, a ser apurada em processo administrativo disciplinar, sujeitando o infrator às penalidades previstas no art. 127 da Lei n. 8.112, de 11 de dezembro de 1990, sem prejuízo da responsabilidade penal e civil.

§ 2º A liberação do uso do serviço de correio eletrônico após a limitação de que trata o inciso II do caput será determinada pelo Comitê Gestor do Serviço de Correio Eletrônico até o primeiro dia útil após:

I – o prazo constante no ato que autorizou a limitação;

II – ciência de determinação expressa do presidente do Tribunal.

Art. 18. Na definição de limites operacionais ao sistema, o Comitê Gestor do Serviço de Correio Eletrônico observará os seguintes aspectos técnicos:

I – espaço físico destinado às caixas postais;

II – tamanho máximo de mensagens internas e externas;

III – número máximo de destinatários para cada mensagem a ser enviada;

IV – tipos de arquivo cujo envio ou recebimento sejam permitidos pelo serviço de correio eletrônico.

Parágrafo único. Será adotada a seguinte política quanto ao limite relacionado com o espaço físico de armazenamento destinado às caixas postais:

I – inicialmente, será enviada, de forma automática, mensagem de alerta ao proprietário da caixa postal a fim de indicar que o limite foi atingido;

II – caso não haja providências e o espaço da caixa postal continue a crescer, o envio de mensagens a partir do endereço de correio eletrônico do proprietário será restringido;

III – se o espaço atingir valores críticos de capacidade, serão bloqueados o envio e o recebimento de mensagens.

Art. 19. As caixas de correio eletrônico individuais poderão ser acessadas por seus titulares de forma remota, a partir de equipamentos externos à rede local do Superior Tribunal de Justiça, nos termos definidos pelo Comitê Gestor do Serviço de Correio Eletrônico.

Art. 20. É facultado ao usuário o serviço de armazenamento local de dados, tal como "pastas particulares".

Parágrafo único. A manutenção dos arquivos a que se refere o caput fica sob a responsabilidade do interessado, o qual deve considerar, no armazenamento de informações críticas ou relevantes, as limitações desses recursos em relação a seus aspectos de integridade e segurança, inerentes à tecnologia atualmente existente.

## CAPÍTULO VIII

## Do Software Utilizado pelo Tribunal

Art. 21. O software utilizado como cliente do sistema de correio eletrônico será apenas aquele homologado pelo Comitê Gestor do Serviço de Correio Eletrônico.

Art. 22. Qualquer aplicativo ou sistema que utilizar o serviço de correio eletrônico somente poderá ser disponibilizado no ambiente da rede local do Tribunal após a homologação da Equipe de Administradores do Correio Eletrônico.

Art. 23. Para assegurar a continuidade da prestação dos serviços da rede local, a Secretaria de Tecnologia da Informação e Comunicação deverá possibilitar o registro de informações sobre o tráfego de dados gerado pelas aplicações, de forma a possibilitar ações preventivas quanto a eventuais colapsos.

## CAPÍTULO IX

## Das Previsões de Acesso às Caixas Postais

Art. 24. O Comitê Gestor do Serviço de Correio Eletrônico fará uso dos recursos tecnológicos e materiais necessários a garantir o cumprimento desta portaria, incluindo a verificação do tráfego, do conteúdo das mensagens transmitidas ou recebidas e dos documentos e demais registros armazenados no sistema de correio eletrônico do Superior Tribunal de Justiça.

§ 1º As verificações previstas no caput ocorrerão nas seguintes situações:

I – por ordem judicial;

II – por necessidade de segregar mensagens não desejadas.

§ 2º Na hipótese prevista no inciso II deste artigo, a filtragem será realizada por programa de computador, sem interferência humana na análise do conteúdo.

§ 3º O Comitê Gestor do Serviço de Correio Eletrônico poderá suspender o acesso a qualquer recurso do serviço de correio eletrônico sempre que julgar necessário, para preservar a confidencialidade, a integridade e a disponibilidade do serviço, bem como para garantir o respeito ao disposto nesta portaria.

Art. 25. Além do próprio gestor de caixa postal ou de pessoas por ele autorizadas, somente o Comitê Gestor do Serviço de Correio Eletrônico poderá acessar o conteúdo das caixas postais, com os seguintes objetivos:

I – recuperar conteúdo de interesse do Tribunal, no caso de afastamento legal do gestor da caixa postal e de seu substituto, exclusivamente quando se tratar do caixa postal da unidade administrativa ou de caixa postal de uso coletivo;

II – atender solicitação judicial.

Parágrafo único. O acesso ao conteúdo de caixas postais nas hipóteses previstas nos incisos I e II deve ser feito mediante autorização do presidente do Tribunal.

## CAPÍTULO X

## Dos Grupos Globais e das Listas de Distribuição

Art. 26. Com a necessária justificativa, poderá ser criada lista de distribuição de mensagens.

Art. 27. A administração das listas de distribuição será realizada:

I – pelo titular da unidade administrativa que a solicitou ou por outra pessoa por ele designada;

II – no caso de grupos independentes, desvinculados das unidades administrativas, pelos seguintes usuários:

a) o líder do grupo interessado;

b) a pessoa designada no ato administrativo que instituiu o grupo.

Art. 28. O servidor que solicitar a criação de grupo será responsável por sua gestão, devendo incluir e, quando necessário, excluir, os endereços dos integrantes da lista.

Art. 29. As listas de distribuição devem ser utilizadas de forma criteriosa, evitando-se envio e recebimento desnecessário de mensagens.

Art. 30. O envio de mensagens para grupos será restrito aos usuários previamente autorizados por seu responsável.

Art. 31. Cabe à Equipe de Administradores do Correio Eletrônico providenciar a exclusão dos grupos globais que caiam em desuso.

## CAPÍTULO XI

## Da Inclusão e da Exclusão de Caixa Postal

Art. 32. As solicitações de criação, ativação, desativação e exclusão de caixa postal individual de usuário interno deverão ser feitas pela Secretaria de Gestão de Pessoas ao Comitê Gestor do Serviço de Correio Eletrônico.

Parágrafo único. A gestão da caixa postal de que trata o caput é de uso e responsabilidade exclusiva do usuário interno associado.

Art. 33. As solicitações de criação, ativação, desativação e exclusão de caixa postal individual de usuário colaborador deverão ser feitas ao Comitê Gestor do Serviço de Correio Eletrônico pela unidade administrativa à qual o usuário colaborador está vinculado ou presta serviço.

§ 1º A necessidade do uso do correio eletrônico corporativo deverá estar prevista em contrato ou em normas institucionais.

§ 2º A gestão da caixa postal a que se refere o caput é de uso e responsabilidade exclusiva do usuário colaborador.

Art. 34. Toda unidade administrativa do Tribunal poderá solicitar ao Comitê

Gestor do Serviço de Correio Eletrônico a criação, ativação, desativação e exclusão de caixa postal associada a ela, sendo o responsável o titular da unidade.

Parágrafo único. A caixa postal de que trata o caput poderá ser acessada por outros usuários, se houver manifestação expressa de seu responsável ao Comitê Gestor do Serviço de Correio Eletrônico.

Art. 35. As solicitações de criação, ativação, desativação e exclusão de caixa postal destinada a grupo de trabalho, comitê, comissão, projeto ou atividade específica de interesse do Tribunal deverão ser encaminhadas ao Comitê Gestor do Serviço de Correio Eletrônico.

Parágrafo único. As solicitações de que trata o caput deverão conter as seguintes informações:

I – usuário interno responsável pela caixa postal;

II – usuários que terão acesso à caixa postal, especificando os direitos de acesso;

III – objetivo a que se destina;

IV – período pelo qual ficará ativa.

Art. 36. A caixa postal será considerada inativa caso ocorra uma das seguintes hipóteses:

I – transcurso de seis meses sem qualquer acesso;

II – cessação do vínculo com o Superior Tribunal de Justiça;

III – aposentadoria de servidor;

IV – usuário especial desligado de função no Tribunal.

§ 1º Na hipótese prevista no inciso I, a caixa postal e seu conteúdo serão excluídos do sistema de correio eletrônico.

§ 2º Na hipótese prevista no inciso III, as mensagens recebidas pelo sistema de correio eletrônico do Tribunal serão encaminhadas ao endereço de correio eletrônico informado pelo interessado pelo período máximo de seis meses.

Art. 37. A exclusão de caixas postais individuais destinadas a servidores ocorrerá imediatamente após a respectiva vacância do quadro do Tribunal, exceto no caso de aposentadoria.

Parágrafo único. Cabe à Secretaria de Gestão de Pessoas informar ao Comitê Gestor do Serviço de Correio Eletrônico as aposentadorias e as demais ocorrências de vacância, para adequação ou exclusão da caixa postal do servidor.

Art. 38. A criação e a exclusão de caixa postal para usuários colaboradores devem seguir as regras previstas no contrato, cabendo à unidade gestora do contrato promover ações necessárias com o intuito de informar ao Comitê Gestor do Serviço de Correio Eletrônico quanto à necessidade de inclusão e exclusão de caixa postal.

§ 1º Cessada a prestação do serviço terceirizado, compete à unidade gestora do contrato requerer ao Comitê Gestor do Serviço de Correio Eletrônico a imediata exclusão das caixas postais dos respectivos usuários colaboradores.

§ 2º Findo o contrato do estágio, compete à Secretaria de Gestão de Pessoas requerer ao Comitê Gestor do Serviço de Correio Eletrônico a imediata exclusão das caixas postais dos respectivos usuários colaboradores.

## CAPÍTULO XII

## Das Disposições Finais

Art. 39. Os casos omissos serão examinados pelo Comitê Gestor do Serviço de Correio Eletrônico e submetidos à deliberação do diretor-geral da Secretaria do Tribunal.

Art. 40. Fica invalidada a Portaria n. 441 de 5 de novembro de 2012.

Art. 41. Esta portaria entra em vigor na data de sua publicação.

**RESOLUÇÃO N. 20 DE 9 DE AGOSTO DE 2012**

Dispõe sobre a certificação digital no Superior Tribunal de Justiça e dá outras providências.

O **PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA,** usando da atribuição que lhe é conferida pelo art. 21, inciso XX, do Regimento Interno e considerando o disposto na Lei n. 11.419, de 19 de dezembro de 2006, e o decidido pelo Conselho de Administração na sessão de 2 de agosto de 2012, Processo STJ n.10421/2010,

**RESOLVE:**

Art. 1º Estabelecer procedimentos para a emissão, utilização e revogação de certificado digital no Superior Tribunal de Justiça.

Art. 2º O certificado digital será emitido para utilização nos atos praticados por magistrados e servidores no exercício de suas funções.

Parágrafo único. Para a utilização em equipamento servidor de rede, poderá ser emitido certificado digital, desde que devidamente justificada pela área de tecnologia da informação.

Art. 3º Para os efeitos desta resolução, entende-se por:

I – assinatura eletrônica: registro realizado eletronicamente por usuário identificado de modo inequívoco com vistas a firmar determinado documento com sua assinatura;

II – autoridade certificadora: entidade autorizada a emitir, expedir, distribuir, revogar e gerenciar os certificados e as correspondentes chaves criptográficas, bem como a disponibilizar aos usuários listas de certificados revogados e manter registros de suas operações;

III – autoridade de registro: entidade operacional vinculada a determinada autoridade certificadora autorizada a identificar e cadastrar usuários, a encaminhar

solicitação de certificados às autoridades certificadoras e a manter registros de suas operações;

IV – mídia de armazenamento do certificado digital: dispositivo portátil – como o *token* – que contém um par de chaves criptográficas e o certificado digital, a ser inserido no computador para a efetivação da assinatura digital;

V – certificado digital: arquivo eletrônico que contém dados de uma pessoa ou de uma instituição e uma chave criptográfica, utilizado para comprovar identidade em ambiente computacional;

VI – usuário interno: magistrado ou servidor que tenha acesso, de forma autorizada, a aplicações e informações produzidas ou custodiadas pelo Tribunal.

Art. 4º Os documentos eletrônicos produzidos no Tribunal terão garantia de autoria, autenticidade e integridade assegurada nos termos da lei, mediante a utilização de assinatura eletrônica em uma das seguintes modalidades:

I – assinatura digital baseada em certificado digital; ou

II – assinatura mediante usuário cadastrado no Superior Tribunal de Justiça.

§ 1° O certificado digital a ser utilizado nos termos do inciso I deve ser emitido por autoridade certificadora aprovada pela Infraestrutura de Chaves Públicas Brasileiras (ICPBrasil).

§ 2º Em caso de impossibilidade técnica, os documentos poderão ser produzidos em papel e assinados de próprio punho pela pessoa competente, devendo a versão em papel, assim que possível, ser digitalizada e assinada eletronicamente, conforme os incisos I ou II.

§ 3º Qualquer servidor ativo poderá certificar documentos eletrônicos resultantes de digitalização, quando solicitado, por meio de uma das assinaturas eletrônicas descritas nos incisos I e II; o credenciamento para esse efeito dar-se-á mediante o procedimento de identificação presencial do interessado nos termos da lei.

Art. 5º O Tribunal proverá os usuários internos de certificado digital e da respectiva mídia de armazenamento; a opção pela assinatura digital é excludente da assinatura de que trata o inciso II do art. 4º.

§ 1º A emissão de certificados digitais será realizada na medida da necessidade do serviço e da implantação das funcionalidades tecnológicas que exigirem seu uso.

§ 2º Caberá ao titular de unidade de nível CJ-3 ou superior solicitar autorização para a emissão de certificado digital.

§ 3º Os procedimentos para a emissão de certificado digital serão realizados mediante autorização do diretor-geral, em formulário específico, com validade de 90 dias a contar da assinatura.

§ 4º O certificado digital de uso pessoal de ministro do Tribunal será solicitado por ele e encaminhado pelo diretor-geral.

Art. 6º O certificado digital é de uso pessoal, intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado nos termos da legislação em vigor, observado o disposto no parágrafo único do art. 2º.

§ 1º O detentor de certificado digital será responsável por sua utilização, guarda e conservação.

§ 2º A prática de atos assinados eletronicamente importará aceitação das normas regulamentares sobre o assunto e da responsabilidade pela utilização indevida da assinatura eletrônica.

§ 3º O usuário do certificado digital não poderá negar a autoria da operação, ficando a ela vinculado.

§ 4º O uso inadequado do certificado digital ficará sujeito à apuração de responsabilidade penal, civil e administrativa na forma da legislação em vigor.

Art. 7º O certificado digital será inutilizado nas seguintes situações:

I – digitação sucessiva de senha incorreta na tentativa de utilização do certificado;

II – dano ou formatação da mídia que armazena o certificado;

III – esquecimento da senha de utilização do certificado;

IV – perda ou extravio;

V – vacância de magistrado ou servidor.

Parágrafo único. A inutilização poderá ser realizada automaticamente por solução de TI ou mediante solicitação.

Art. 8º O extravio, ou dano, do dispositivo de armazenamento com certificado digital deverá ser imediatamente comunicado à unidade de tecnologia da informação e comunicação e implicará o ressarcimento, por parte do usuário responsável, do custo de reposição de novo instrumento.

§ 1º O custo será estabelecido por meio de portaria do diretor-geral.

§ 2º O ressarcimento das despesas com a emissão de novo instrumento de identificação será feito mediante débito em folha de pagamento.

§ 3º A formalização do comunicado de que trata o *caput* será feita por meio do preenchimento de formulário específico.

Art. 9º Compete às unidades de gestão de pessoas, no que se refere a servidores, e à de atendimento aos ministros, no que concerne a magistrados:

I – conferir os dados cadastrais constantes das solicitações de autorização para emissão de certificado digital das unidades do Tribunal;

II – informar à unidade de tecnologia da informação e comunicação o desligamento de magistrados e servidores com vistas ao recebimento do termo de devolução de dispositivo de armazenamento com o certificado digital;

III – informar à unidade de tecnologia da informação e comunicação a mudança de lotação para que seja verificada a necessidade de permanência da certificação.

Art. 10. Compete à unidade de tecnologia da informação e comunicação no âmbito de suas atribuições:

I – receber e analisar as solicitações de autorização para a emissão de certificado digital sob o ponto de vista tecnológico, após a análise contida no inciso I do art. 9º, a serem encaminhadas ao diretor-geral para aprovação;

II – adotar providências para a emissão e distribuição de certificados digitais, mediante registro e controle;

III – adequar a infraestrutura de TI para uso dos certificados digitais;

IV – elaborar procedimentos para a emissão, renovação, revogação e reemissão de certificados digitais;

V – divulgar diretrizes para a criação de senhas de acesso ao certificado que dificultem ao máximo sua dedução;

VI – monitorar e avaliar periodicamente as práticas de segurança da informação relativas ao uso dos certificados digitais e propor os ajustes que considerar necessários;

VII – elaborar padrões de compatibilidade de certificados digitais e das respectivas mídias de armazenamento utilizados no Tribunal;

VIII – prover solução de TI para gerenciar o ciclo de vida dos certificados digitais dos usuários internos do Tribunal;

IX – apresentar termo de devolução de certificado digital e de dispositivo de armazenamento dos usuários internos – magistrados e servidores – à unidade competente;

X – desenvolver, em sua área de atuação, outras atividades relativas ao uso dos certificados digitais;

XI – solicitar autorização para a emissão e a distribuição do certificado digital e gerenciar seu ciclo de vida para equipamento servidor de rede sob a responsabilidade da respectiva unidade provedora do serviço.

Art. 11. Compete aos usuários internos detentores de certificado digital:

I – apresentar, tempestivamente, à autoridade certificadora a documentação necessária à emissão do certificado digital;

II – estar de posse do certificado digital para o desempenho de atividades funcionais que requeiram seu uso;

III – fornecer informações solicitadas para a emissão, utilização e revogação;

IV – solicitar a imediata revogação do certificado em caso de inutilização;

V – alterar, imediatamente, a senha de acesso ao certificado em caso de suspeita de seu conhecimento por terceiro;

VI – observar as diretrizes definidas para a criação e utilização de senhas de acesso ao certificado;

VII – manter a mídia de armazenamento dos certificados digitais em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor excessivo e outras condições ambientais que representem risco à integridade dessas mídias;

VIII – solicitar o fornecimento de nova mídia de armazenamento nos casos de extravio ou dano e de certificado digital quando inutilizado, revogado ou expirado, se for o caso;

IX – verificar, periodicamente, a data de validade do certificado e solicitar, tempestivamente, a emissão de novo certificado;

X – devolver o dispositivo de armazenamento com certificado digital Parágrafo único. A vacância do cargo de magistrado e de servidores implica devolução ao Tribunal do certificado digital e da respectiva mídia de armazenamento, anteriormente distribuído ao usuário interno, para fins de inutilização do certificado e formatação da mídia.

Art. 12. Cabe ao diretor-geral editar os atos que se fizerem necessários ao cumprimento desta resolução.

Art. 13. Os casos omissos serão resolvidos pelo presidente.

Art. 14. Esta resolução entra em vigor na data de sua publicação

**RESOLUÇÃO N. 8, DE 13 DE NOVEMBRO DE 2009.**

O **PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA**, no uso da atribuição que lhe é conferida pelo Regimento Interno, art. 21, XX, e tendo em vista o decidido pelo Conselho de Administração em sessão de 4 de novembro de 2009, e no Processo Administrativo STJ n. 4.144/2009,

**RESOLVE**:

Art. 1º Instituir o Código de Conduta do Superior Tribunal de Justiça, com as seguintes finalidades:

I – tornar claras as regras de conduta dos servidores e gestores do Tribunal;

II – assegurar que as ações institucionais empreendidas por gestores e servidores do Tribunal preservem a missão deste e que os atos, delas decorrentes, reflitam probidade e conduta ética;

III – conferir coerência e convergência às políticas, diretrizes e procedimentos internos do Tribunal;

IV – oferecer um conjunto de atitudes que orientem o comportamento e as decisões institucionais;

Art. 2º O Código de Conduta do Superior Tribunal de Justiça aplicar-se-á a todos os servidores e gestores do Tribunal que deverão observá-lo e firmar Termo de Compromisso declarando ciência e adesão.

Parágrafo único: Cabe aos gestores, em todos os níveis, aplicar e garantir que seus subordinados – servidores, estagiários e prestadores de serviço - apliquem os preceitos estabelecidos neste Código, como um exemplo de conduta a ser seguido por todos.

Art. 3º O Código de Conduta do Superior Tribunal de Justiça integrará todos os contratos de estágio e de prestação de serviços de forma a assegurar o alinhamento entre todos os colaboradores do Tribunal.

Art. 4º A conduta dos destinatários deste Código deverá ser pautada pela integridade, pela lisura, pela transparência, pelo respeito e pela moralidade.

Art. 5º O Superior Tribunal de Justiça não será tolerante com atitudes discriminatórias ou preconceituosas de qualquer natureza relativamente à etnia, sexo, religião, estado civil, orientação sexual, faixa etária ou condição física especial, nem comatos que caracterizem proselitismo partidário, intimidação, hostilidade ou ameaça, humilhações por qualquer motivação, assédio moral e sexual.

Art. 6º Gestores ou servidores não poderão participar de atos ou circunstâncias que se contraponham ao interesse do Tribunal ou possam lhe causar dano ou prejuízo.

Art. 7º Recursos, espaço e imagem do Tribunal não poderão, sob qualquer hipótese, ser usados para atender a interesses pessoais, políticos ou partidários.

Art. 8º O servidor ou gestor que, por força de seu cargo ou de suas responsabilidades, tenha acesso a informações do Tribunal ainda não divulgadas publicamente, deverá manter sigilo sobre seu conteúdo.

Art. 9º Ao servidor ou gestor do Tribunal é vedado aceitar presentes, privilégios, empréstimos, doações, serviços ou qualquer outra forma de benefício, em seu nome ou de seus familiares, quando originários de partes, ou dos respectivos advogados e estagiários, bem como de terceiros que sejam ou pretendam ser fornecedores de produtos ou serviços para o Tribunal.

Parágrafo único: Não se consideram presentes, para fins deste artigo, os brindes sem valor comercial ou aqueles distribuídos por entidades de qualquer natureza, a título de cortesia, propaganda ou divulgação, por ocasião de eventos especiais ou datas comemorativas.

Art. 10 É de responsabilidade dos destinatários deste Código, zelar pela integridade dos bens do Tribunal, tangíveis e intangíveis, inclusive sua reputação, propriedade intelectual e informações confidenciais, estratégicas ou sensíveis.

Art. 11 Os recursos de comunicação e tecnologia da informação disponíveis no Tribunal devem ser utilizados com a estrita observância dos normativos internos vigentes, notadamente no que tange à utilização e à proteção

das senhas de acesso. É vedada, ainda, a utilização de sistemas e ferramentas de comunicação para a prática de atos ilegais ou impróprios, para obtenção de vantagem pessoal, para acessar ou divulgar conteúdo ofensivo ou imoral, para interferir em sistemas de terceiros e para participar de discussões virtuais acerca de assuntos não relacionados aos interesses do Tribunal.

Art. 12 A comunicação entre os destinatários deste Código ou entre estes e os órgãos governamentais, clientes, fornecedores e sociedade deve se dar de forma indiscutivelmente clara, simples, objetiva e acessível a todos os legitimamente interessados.

Art. 13 É obrigatório aos servidores e gestores do Tribunal garantir a publicidade de seus atos e a disponibilidade de informações corretas e atualizadas que permitam o conhecimento dos aspectos relevantes da atividade sob sua responsabilidade, bem como assegurar que a divulgação das informações aconteça no menor prazo e pelos meios mais rápidos.

Art. 14 Os contatos com os órgãos de imprensa serão promovidos, exclusivamente pelos porta-vozes autorizados pelo Tribunal.

Art. 15 Os investimentos de qualquer natureza, inclusive aqueles destinados à capacitação de servidores e gestores devem ser, necessariamente, orientados pelas reais demandas do Tribunal.

Art. 16 Os contratos, convênios ou acordos de cooperação nos quais o Superior Tribunal de Justiça tome parte devem ser escritos de forma clara, com informações precisas, sem que haja possibilidade de interpretações ambíguas por qualquer das partes interessadas.

Art. 17 Eventuais erros cometidos por servidores ou gestores do Tribunal deverão receber orientação construtiva, mas falhas resultantes de desídia, má fé, negligência ou desinteresse que exponham o Tribunal a riscos legais ou de imagem, serão tratadas com rigorosa correção.

Art. 18 O Superior Tribunal de Justiça exige de seus servidores, no exercício de seus misteres, a responsabilidade social e ambiental; no primeiro caso, privilegiando a adoção de práticas que favoreçam a inclusão social e, no segundo, de práticas que combatam o desperdício de recursos naturais e evitem danos ao meio ambiente.

Art. 19 Fica instituído o Comitê Gestor do Código de Conduta que deverá, entre outras atribuições, zelar pelo seu cumprimento.

Art. 20 As atribuições do Comitê Gestor do Código de Conduta bem como a designação de seus integrantes será formalizada por ato do Presidente do Tribunal.

Art. 21 Esta resolução entra em vigor na data de sua publicação.

Ministro CESAR ASFOR ROCHA

## ANEXO C: PSIC do Tribunal Superior Eleitoral

**RESOLUÇÃO Nº 22.780**

(24 DE ABRIL DE 2008)

*Publicada no DJU de 27.6.2008.*

Processo Administrativo nº 19.878 – Classe 19ª - Brasília - Distrito Federal
Relator: Ministro Joaquim Barbosa
Interessado: Tribunal Superior Eleitoral

Estabelece princípios e valores a serem adotados para assegurar a integridade, a confidencialidade e a disponibilidade das informações no âmbito da Justiça Eleitoral.

O Tribunal Superior Eleitoral, no uso de suas atribuições, resolve expedir diretrizes visando a regulamentar a Política de Segurança da Informação da Justiça Eleitoral:

### CAPÍTULO I
### DAS DEFINIÇÕES

**Art. 1º** Para os efeitos desta resolução aplicam-se as seguintes definições:

I - atividades críticas: conjunto de processos vinculados às atividades precípuas da Justiça Eleitoral, cuja interrupção ocasiona severos transtornos;

II - atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade fim da Justiça Eleitoral, contemplando todos os ambientes existentes, no âmbito do Tribunal Superior Eleitoral e tribunais regionais eleitorais;

III - ativo de informação: é o patrimônio composto por todos os dados e informações geradas, adquiridas, utilizadas ou armazenadas pela Justiça Eleitoral;

IV - ativo de processamento: é o patrimônio composto por todos os elementos de *hardware*, *software* e infraestrutura de comunicação, necessários para a execução das atividades precípuas da Justiça Eleitoral;

V - confidencialidade: a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

VI - criticidade: grau de importância da informação, para a continuidade das atividades precípuas da Justiça Eleitoral;

VII - disponibilidade: a informação será acessível e utilizável sob demanda da entidade autorizada;

VIII - integridade: proteção à precisão e à perfeição de recursos;

IX - recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

X - usuário: quem utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XI - segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.

## CAPÍTULO II
## DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 2º A Política de Segurança da Informação da Justiça Eleitoral (PSI) deve ser empregada para preservação da integridade, confidencialidade e credibilidade dos ativos de informação da Justiça Eleitoral.

Art. 3º A Política de Segurança da Informação da Justiça Eleitoral visa a combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações.

Art. 4º A Política de Segurança da Informação da Justiça Eleitoral (PSI) se aplica a todos os servidores, estagiários e prestadores de serviço, que fazem uso dos recursos materiais e tecnológicos.

Parágrafo único. Todos os servidores, estagiários e prestadores de serviço da

Justiça Eleitoral são co-responsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir a Política de Segurança da Informação da Justiça Eleitoral.

## CAPÍTULO III

## DA SEGURANÇA DA INFORMAÇÃO

Art. 5º A fim de preservar a continuidade, integridade e disponibilidade das informações e serviços devem ser adotados mecanismos de proteção.

Art. 6º Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Justiça Eleitoral é considerada de sua propriedade e deve ser protegida, de acordo com a Política de Segurança da Informação de que trata esta resolução, legislação em vigor e com as normas e procedimentos relacionados.

Art. 7º As informações devem ser classificadas de acordo com um sistema próprio, determinado pela necessidade de sigilo, confidencialidade e disponibilidade, para garantir o armazenamento, a proteção de acesso e o uso adequado.

Parágrafo único. Os sistemas e equipamentos utilizados para armazenamento de informações devem receber a mesma classificação dada à informação neles mantida.

Art. 8º Deverão ser realizadas auditorias periódicas dos ativos da Justiça Eleitoral, de forma a aferir o correto cumprimento da Política de Segurança da Informação.

## CAPÍTULO IV

## DA INSTITUIÇÃO DAS COMISSÕES DE SEGURANÇA DA INFORMAÇÃO

Art. 9º Deverá ser constituída, no âmbito de cada tribunal eleitoral, comissão de segurança da informação, composta, no mínimo, por representantes da Diretoria-Geral, da Corregedoria, da Secretaria de Gestão de Pessoas e da Secretaria de Tecnologia da Informação.

Parágrafo único. As comissões de segurança da informação constituídas no âmbito de cada tribunal regional deverão acompanhar as diretrizes estabelecidas pela Comissão de Segurança da Informação do TSE.

## CAPÍTULO V

## DO USO DE RECURSOS TECNOLÓGICOS

Art. 10. No que se refere à segurança da informação, é proibido tudo aquilo que não esteja expressamente autorizado pela Comissão de Segurança da Informação.

Art. 11. É vedado o uso de recursos da Justiça Eleitoral para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, bem como para veicular opiniões político-partidárias.

Art. 12. É vedado que apenas um usuário possua controle exclusivo de um processo de negócio ou recurso.

Art. 13. Todos os ativos de informação ou processamento da Justiça Eleitoral devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 14. Cada ativo deverá ter um gestor formalmente designado.

Art. 15. Qualquer indício de falha na segurança da informação deve ser formalmente registrado e notificado ao gestor do ativo, bem como à comissão de segurança da informação de seu respectivo tribunal.

## CAPÍTULO VI

## DOS USUÁRIOS DE RECURSOS TECNOLÓGICOS

Art. 16. Todo usuário deve possuir identificação pessoal, intransferível e com validade estabelecida.

Art. 17. Deverão ser adotados mecanismos que garantam a integridade e autenticidade da identificação do usuário.

Art. 18. O usuário receberá permissão de acesso apenas aos recursos necessários e indispensáveis ao desempenho de suas funções.

Parágrafo único. As permissões de acesso deverão ser bloqueadas, em caso de afastamento provisório de fato, e revogadas, em caso de desligamento do usuário.

## CAPÍTULO VII

## DO GERENCIAMENTO DE RISCOS

Art. 19. Deverá ser implementado processo de gerenciamento de riscos, visando à identificação e à mitigação de riscos associados às atividades críticas da Justiça Eleitoral.

Parágrafo único. O processo de gerenciamento de riscos deverá ser revisado periodicamente.

Art. 20. Deverão ser elaborados planos de continuidade de negócio para cada atividade crítica, de forma a garantir o fluxo das informações necessárias em momento de crise e o retorno seguro à situação de normalidade.

Parágrafo único. Os planos de continuidade de negócio deverão ser testados e revisados periodicamente.

## CAPÍTULO VIII

## DAS COMPETÊNCIAS

Art. 21. Compete à Diretoria-Geral de cada tribunal integrante da Justiça Eleitoral apoiar a aplicação das ações estabelecidas na Política de Segurança da Informação e normas correlatas.

Art. 22. Compete à Comissão de Segurança da Informação do Tribunal Superior Eleitoral:

I - analisar criticamente e submeter a Política de Segurança da Informação da Justiça Eleitoral à aprovação da Corte;

II - avaliar as mudanças impactantes na exposição dos recursos a riscos,

identificando as principais ameaças;

III - analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas;

IV - propor iniciativas para aumentar o nível da segurança da informação;

V - promover a divulgação da Política da Segurança da Informação, bem como

ações para disseminar a cultura em segurança da informação;

VI - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios;

VII - promover ações com o propósito de viabilizar recursos para o cumprimento da Política da Segurança da Informação;

VIII - definir planos para realizações de auditorias periódicas.

Art. 23. Compete às comissões de segurança da informação dos tribunais regionais eleitorais:

I - avaliar as mudanças impactantes na exposição dos recursos a riscos, identificando as principais ameaças;

II - analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas;

III - propor iniciativas para aumentar o nível da segurança da informação;

IV - promover a divulgação da Política da Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação;

V - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios;

VI - promover ações, com o propósito de viabilizar recursos para o cumprimento da Política da Segurança da Informação;

VII - definir o plano de auditoria periódica, no âmbito do Tribunal Eleitoral a que estiver vinculada.

Art. 24. Compete às Secretarias de Tecnologia da Informação:

I - prover o apoio necessário à implementação e compreensão da Política de Segurança da Informação da Justiça Eleitoral;

II - executar as orientações técnicas e procedimentos estabelecidos pela comissão de segurança da informação do seu respectivo tribunal;

III - prover os ativos de processamento necessários ao cumprimento da Política da Segurança da Informação;

IV - subsidiar a comissão de segurança da informação do seu respectivo tribunal com informações de cunho tecnológico, aplicadas à execução da Política da Segurança da Informação;

V - apoiar a realização de auditorias, conforme plano de auditoria periódica.

Art. 25. Compete aos usuários:

I - responder por toda atividade executada com o uso de sua identificação;

II - ter pleno conhecimento e seguir a Política de Segurança da Informação;

III - notificar a sua chefia imediata e à Comissão de Segurança da Informação qualquer indício ou falha na segurança da informação.

## CAPÍTULO IX

## DISPOSIÇÕES FINAIS

Art. 26. Fica assegurado às comissões de segurança da informação, a qualquer tempo, o poder de suspender temporariamente o acesso do usuário a recurso computacional da Justiça Eleitoral, quando evidenciados riscos à segurança da informação.

Art. 27. Caberá à Comissão de Segurança da Informação do Tribunal Superior Eleitoral elaborar, revisar, atualizar, divulgar e validar as diretrizes, normas, procedimentos e instruções, que regulamentem os princípios e valores existentes na Política de Segurança da Informação, bem como referendar as proposições encaminhadas pelas comissões de segurança da informação dos tribunais regionais eleitorais.

Art. 28. As atividades das comissões de segurança da informação devem ser executadas em conformidade com as recomendações publicadas pela Associação

Brasileira de Normas Técnicas - ABNT - relativas a sistemas de gestão de segurança da informação.

Art. 29. Compete às comissões de segurança da informação de cada tribunal eleitoral a elaboração de normas e procedimentos visando à regulamentação e operacionalização das diretrizes apresentadas nesta resolução.

Parágrafo único. As normas e procedimentos de que trata o caput desse artigo deverão ser elaboradas tomando-se por base os objetivos de controle e controles estabelecidos na NBR ISO IEC 17799:2005, quais sejam:

I - organização da segurança da Informação;

II - gestão de ativos;

III - segurança em recursos humanos;

IV - segurança física e do ambiente;

V - gerenciamento das operações e comunicações;

VI - controles de acessos;

VII - aquisição, desenvolvimento e manutenção de sistemas de informação;

VIII - gestão de incidentes de segurança da informação;

IX - gestão da continuidade do negócio; e

X - conformidade.

Art. 30. Os casos omissos serão resolvidos pelas comissões de segurança da informação.

Art. 31. Esta resolução entrará em vigor na data de sua publicação.

Marco Aurélio - Presidente. Joaquim Barbosa - Relator. Carlos Ayres Britto. Ari Pargendler. Felix Fischer. Marcelo Ribeiro. Arnaldo Versiani.

Brasília, 24 de abril de 2008.

*Publicada no DJU de 27.6.2008.*

## ANEXO D: PSIC do Tribunal Superior do Trabalho

**TRIBUNAL SUPERIOR DO TRABALHO**
**PRESIDÊNCIA**

**ATO Nº 764/GDGSET.GP, DE 27 DE NOVEMBRO DE 2012**

Estabelece as diretrizes de segurança da informação no âmbito do Tribunal Superior do Trabalho.

O **PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO**, no uso de suas atribuições legais e regimentais,

Considerando o Ato TST.GP. nº 493/2009, que cria o Comitê Gestor de Segurança da Informação e define suas competências no âmbito do Tribunal Superior do Trabalho;

Considerando o Ato TST.GDGSET.GP. nº 86/2010, que define os papéis e as responsabilidades de Área Gestora, Gestor, Gerente e Operador de Sistemas Informatizados e de Bases de Dados no âmbito do Tribunal Superior do Trabalho;

Considerando que a NBR ISO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

Considerando as recomendações da Secretaria de Fiscalização de Tecnologia da Informação referentes à segurança da informação publicadas nos acórdãos do Tribunal de Contas da União;

Considerando as melhores práticas para a proteção e controle da informação referenciadas nas disciplinas do COBIT, ITIL, NBR ISO/IEC 17799 e a família de normas NBR ISO/IEC 27000, seguidas pelas principais organizações e órgãos governamentais;

Considerando a necessidade de ampliar as diretrizes e os padrões de segurança para garantir um ambiente tecnológico controlado e seguro, de forma a oferecer as informações necessárias aos processos de trabalho deste Tribunal com integridade, confidencialidade e disponibilidade;

Considerando a necessidade de regular a concessão de acessos aos sistemas informatizados e à rede de computadores; o uso da Internet e seus recursos; a utilização do serviço de correio eletrônico corporativo; bem como o controle, monitoramento e auditoria de segurança da informação no âmbito do Tribunal;

Considerando os danos potenciais decorrentes da instalação de programas não homologados e inadequados, bem como o risco de disseminação de vírus de computador a partir das estações de trabalho e de dispositivos móveis;

Considerando o contido no Processo Administrativo nº 500.459/2012-7;

**RESOLVE**:

Art. 1º. Este Ato define a Política de Segurança da Informação do Tribunal Superior do Trabalho, cabendo aos usuários a observância de suas disposições e às unidades administrativas, no âmbito de suas competências, a implementação e o acompanhamento de ações para a segurança da informação.

Art. 2º. Para efeitos deste aplicam-se as seguintes definições:

I – Confidencialidade: princípio de segurança da informação que garante o acesso à informação somente a usuários autorizados;

II – Integridade: princípio de segurança da informação que salvaguarda a exatidão e a completeza da informação e dos métodos de processamento;

III – Disponibilidade: princípio de segurança da informação que garante aos usuários autorizados acesso à informação e aos ativos correspondentes;

IV – Ativos de informação: patrimônio composto por pessoas, por elementos de infraestrutura tecnológica (hardware e software), bem como pelos dados e informações gerados e manipulados nos processos de trabalho do Tribunal;

V – Controle de acesso: conjunto de recursos que efetivam as autorizações e as restrições de acesso aos ativos de informação;

VI – Ambiente computacional ou informatizado: conjunto de recursos que utiliza ou disponibiliza serviços de tecnologia da informação e sistemas de informação do Tribunal;

VII – Análise de risco e vulnerabilidades: avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de sua ocorrência;

VIII – Usuários: conjunto composto por ministros, servidores, prestadores de serviço e estagiários no exercício de suas funções públicas, para fins de segurança da informação, que tenham acesso aos recursos de Tecnologia da Informação sob responsabilidade da SETIN, divididos da seguinte forma:

a. Usuário interno: ministro, servidor ativo ou unidade do Tribunal;

b. Usuário inativo: ministro aposentado, servidor aposentado ou pensionista;

c. Usuário colaborador: prestador de serviço terceirizado, estagiário ou outro colaborador do Tribunal;

d. Usuário externo: pessoa física ou jurídica;

IX – Sítio: é um conjunto de páginas web, isto é, de hipertextos acessíveis, geralmente, pelo protocolo HTTP ou HTTPS na Internet. Também conhecido por site, sítio na Internet, website, etc;

X – SPAM: termo usado para referir-se aos e-mails não solicitados e indesejados, que são enviados para um grande número de pessoas;

XI – Programa de computador: conjunto de instruções em linguagem natural ou codificada executado por computador; dispositivos; instrumentos ou equipamentos periféricos, baseados em técnica digital ou analógica, para fazê-los funcionar de modo e para fins determinados;

XII – Licença de uso: cessão de direito de utilização do programa de computador, outorgada pelo detentor dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado, mediante pagamento único ou periódico;

XIII – Programa de terceiro: programa que não foi elaborado por equipe de informática da SETIN;

XIV – Programa de livre distribuição: programa que oferece período de avaliação gratuito, após o qual é requerido pagamento pela licença de uso, ou que pode ser utilizado gratuitamente por tempo indeterminado.

XV – Vírus: programas criados para causar algum dano ao computador infectado, seja apagando dados, capturando informações ou alterando o funcionamento normal da máquina;

XVI – Conteúdo evasivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a saída de informações ou dados;

XVII – Conteúdo intrusivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a entrada de informações ou dados.

## CAPÍTULO I

## DO CONTROLE DE ACESSO À REDE DE COMPUTADORES

Art. 3º. Os serviços de acesso à rede de computadores do Tribunal abrangem: estrutura de diretórios de rede, Intranet, Internet e correio eletrônico.

Parágrafo único. O acesso padrão à rede de computadores do Tribunal é assim regulado:

I – Para usuário interno: será facultado o acesso a toda rede de computadores do Tribunal;

II – Para usuário inativo: será permitido o acesso à Intranet e ao correio eletrônico do Tribunal;

III – Para usuários colaboradores e externos: será facultado o acesso a rede de computadores do Tribunal, sendo vedada a utilização de Internet e o envio ou o recebimento de mensagens externas de correio eletrônico.

Art. 4°. A solicitação de concessão de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço.

§ 1° Na solicitação de acesso à rede de computadores do Tribunal para usuários internos, constará nome completo e código do usuário interessado, bem como os serviços solicitados, conforme descritos no art. 3º.

§ 2° No caso de usuários colaboradores ou externos, a solicitação conterá ainda o tempo de validade do acesso à rede de computadores do Tribunal, sendo o limite a duração do estágio ou do contrato.

§ 3° A SETIN poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso concedido ao usuário.

Art. 5º. O acesso à rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 6°. O acesso à rede de computadores do Tribunal e seus serviços dar-se-á pela combinação nome de usuário e senha, que é pessoal e intransferível.

§ 1° A senha deverá ter um tamanho mínimo de 6 (seis) caracteres alfanuméricos, devendo ser evitada aquela de fácil dedução.

§ 2° A senha de acesso à rede de computadores do Tribunal será alterada com a periodicidade de 45 (quarenta e cinco) dias.

§ 3° O sistema impedirá o usuário de reutilizar as suas 5 (cinco) últimas senhas.

Art. 7°. A solicitação de revogação de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço, quando houver o desligamento do usuário de sua unidade.

## CAPÍTULO II

## DO CONTROLE DE ACESSO AOS SISTEMAS INFORMATIZADOS E AOS BANCO DE DADOS

Art. 8º. A solicitação de concessão de acesso aos sistemas informatizados do Tribunal será encaminhada pelo responsável da unidade ao gestor do respectivo sistema.

§ 1° Na solicitação de acesso aos sistemas informatizados do Tribunal, deverá constar nome completo e código do usuário interessado, bem como o tipo de acesso a ser concedido.

§ 2° No caso de usuários colaboradores ou externos, a solicitação deverá conter ainda o tempo de validade do acesso aos sistemas informatizados do Tribunal, sendo o limite a duração do estágio ou do contrato.

Art. 9º. O acesso aos sistemas informatizados e aos bancos de dados será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 10. A solicitação de revogação de acesso aos sistemas informatizados do Tribunal será realizada pelo responsável da unidade ao gestor do sistema, quando houver o desligamento do usuário de sua unidade.

Art. 11. Os servidores lotados na Coordenadoria de Desenvolvimento de Sistemas da SETIN poderão ter acesso aos sistemas em produção e aos bancos de dados para realizar manutenções, mediante autorização expressa do gestor do sistema.

Art. 12. O gestor do sistema poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso do usuário ao sistema informatizado do Tribunal.

## CAPÍTULO III

## DO CONTROLE DE ACESSO AO GABINETE VIRTUAL

Art. 13. A solicitação de concessão de acesso ao Gabinete Virtual do Tribunal será realizada pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço.

Parágrafo único. No Gabinete Virtual, o usuário contará o mesmo perfil de acesso que detém na rede de computadores e nos sistemas informatizados do Tribunal.

Art. 14. O acesso realizado pelo Gabinete Virtual será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 15. A solicitação de revogação de acesso ao Gabinete Virtual do Tribunal será realizada pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço, quando houver o desligamento do usuário de sua unidade.

## CAPÍTULO IV

## DO CONTROLE DE ACESSO À INTERNET E À INTRANET

Art. 16. A concessão de acesso à Internet e à Intranet no âmbito do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 17. O acesso à Internet ou à Intranet, partindo de computadores situados no âmbito do Tribunal, será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 18. O uso não apropriado do acesso à Internet e à Intranet será passível de apuração de responsabilidade.

Parágrafo único. Entende-se por uso não apropriado o acesso a sítios ou quaisquer outros serviços:

I – de conteúdo considerado ofensivo, ilegal ou impróprio;

II – do tipo chat, bate-papo e troca de mensagens em tempo real que não tenham sido formalmente autorizados;

III – que apresentem vulnerabilidade de segurança ou possam comprometer a integridade e a disponibilidade da rede de computadores do Tribunal;

IV – que possuem conteúdos evasivos e/ou intrusivos.

Art. 19. A comprovação, por auditoria, do uso não apropriado implicará o bloqueio imediato da Internet para o usuário e a comunicação ao responsável da unidade de lotação do usuário.

Art. 20. Caberá à SETIN, a qualquer momento, o bloqueio de sítios cujo conteúdo seja considerado não apropriado.

Art. 21. É vedada a transferência entre a rede de computadores do Tribunal e a Internet dos seguintes tipos de arquivos:

I – fotos de conteúdos pornográficos;

II – músicas e filmes de qualquer formato;

III – programas ou arquivos executáveis;

IV – programas de conteúdo prejudicial à segurança do ambiente computacional desta Corte.

Art. 22. O acesso à Intranet poderá ser efetuado a partir de computadores que estejam fora das dependências do TST, mediante a combinação nome de usuário e senha da rede de computadores do Tribunal.

Art. 23. A SETIN será responsável pela manutenção da disponibilidade de banda na Internet e pelo seu monitoramento. Caso necessário, poderá estabelecer limites e quotas para a transferência de dados dos usuários.

## CAPÍTULO V

## DO CONTROLE DE ACESSO À REDE SEM FIO – WIRELESS

Art. 24. Os usuários internos deste Tribunal terão acesso à rede sem fio.

Art. 25. A solicitação de concessão de acesso à rede sem fio do Tribunal para usuários colaboradores e externos será feita pelo responsável da unidade, utilizando o Sistema de Solicitação de Serviço.

§ 1° O responsável da unidade assinará o Termo de Responsabilidade, disponibilizado na Intranet.

§ 2° O acesso dos usuários colaboradores e externos será revogado em 180 dias, caso o Termo de Responsabilidade não indique data e justificativa para sua manutenção.

Art. 26. O acesso à rede sem fio será realizado mediante a combinação nome de usuário e senha da rede de computadores do Tribunal.

Art. 27. O acesso efetuado pela rede sem fio do Tribunal deverá atender ao disposto nos capítulos de I a IV deste Ato e será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 28. A solicitação de revogação de acesso à rede sem fio do Tribunal será realizada pelo usuário à SETIN, utilizando o Sistema de Solicitação de Serviço.

Art. 29. A rede sem fio dará acesso à Internet, sendo vedada a comunicação direta com a rede interna do Tribunal.

## CAPÍTULO VI

## DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 30. Os serviços de correio eletrônico corporativo do Tribunal serão destinados às atividades do Tribunal, sendo vedado o seu uso para assuntos particulares.

Art. 31. A concessão de acesso ao correio eletrônico corporativo do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 32. A mensagem enviada ou recebida pelo correio eletrônico corporativo do Tribunal, seja seu destino interno ou externo, deverá primar pelo uso apropriado da ferramenta.

Art. 33. O uso não apropriado do correio eletrônico corporativo do Tribunal é passível de apuração de responsabilidade do usuário.

Parágrafo único. Por uso não apropriado, considera-se o envio de mensagens de correio eletrônico contendo:

I – materiais obscenos, ilegais ou antiéticos;

II – materiais preconceituosos ou discriminatórios;

III – materiais caluniosos ou difamatórios;

IV – propagandas com objetivos comerciais;

V – listas de endereços eletrônicos dos usuários do correio eletrônico corporativo do Tribunal;

VI – vírus ou qualquer programa danoso;

VII – material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

VIII – material protegido por leis de propriedade intelectual;

IX – entretenimentos e “correntes”;

X – assuntos ofensivos;

XI – músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

XII – SPAM.

Art. 34. Ao usuário é permitida a participação em listas de discussão com assuntos relacionados ao interesse do trabalho.

Art. 35. O envio de mensagem eletrônica para listas de endereços eletrônicos do Tribunal deverá ser realizado utilizando o endereço de correio eletrônico corporativo da unidade.

Art. 36. Os anexos das mensagens de correio eletrônico não poderão exceder o tamanho estabelecido em norma interna da SETIN, disponível na Intranet do Tribunal.

Parágrafo único. Será vedado ao usuário o envio de anexo que configure o uso não apropriado do correio eletrônico corporativo, conforme Art. 36, parágrafo único.

Art. 37. O envio e o recebimento de mensagens do correio eletrônico corporativo do Tribunal serão registrados pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 38. A regra de denominação do endereço de correio eletrônico corporativo pessoal será, preferencialmente, o prenome e o sobrenome do servidor, em letras minúsculas, sem acentos, cedilhas ou caracteres especiais, separados pelo sinal de ponto, acrescido do sufixo “@tst.jus.br”.

Parágrafo único. As exceções serão tratadas segundo norma interna da SETIN, disponível na Intranet do Tribunal.

Art. 39. A regra de denominação do endereço de correio eletrônico corporativo das unidades será, preferencialmente, a sigla oficial da unidade no Tribunal, em letras minúsculas, sem acentos, cedilhas, traços, conectivos, pontos ou caracteres especiais, acrescido do sufixo “@tst.jus.br”.

Parágrafo único. O endereço de correio eletrônico corporativo será de uso do responsável pela unidade, admitindo-se a designação de servidores para operá-lo.

Art. 40. As regras previstas nos arts. 38 e 39 deste Ato aplicam-se, no que couber, aos e-mails corporativos pessoais e das unidades criados sob a responsabilidade do Conselho Superior da Justiça do Trabalho – CSJT, com o sufixo "@csjt.jus.br", e da Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho – ENAMAT, com o sufixo "@enamat.gov.br".

Art. 41. As mensagens de correio eletrônico de usuários colaboradores somente poderão ser enviadas ou recebidas para endereços internos do Tribunal. Caso seja necessário o envio e recebimento de mensagens externas, o responsável pela unidade deverá solicitar a alteração à SETIN pelo Sistema de Solicitação de Serviços.

Art. 42. O limite de tamanho das caixas postais corporativas pessoais e das unidades do Tribunal será fixado em norma interna da SETIN, disponível na Intranet do Tribunal.

Art. 43. Será responsabilidade do usuário do correio eletrônico corporativo do Tribunal:

I – utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais;

II – eliminar periodicamente as mensagens contidas nas caixas postais;

III – não permitir acesso de terceiros ao correio eletrônico por meio de sua senha;

IV – notificar a SETIN, por meio do endereço seguranca@tst.jus.br, o recebimento de mensagens inapropriadas, conforme o disposto no Art. 33 deste Ato.

## CAPÍTULO VII

## DA UTILIZAÇÃO DA ESTRUTURA DE DIRETÓRIOS NA REDE DE COMPUTADORES

Art. 44. A concessão de acesso à estrutura de diretórios da rede de computadores do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 45. O usuário da rede de computadores do Tribunal terá acesso a diretório pessoal e restrito – denominado “P:” – e a diretório da unidade onde estiver lotado – denominado “K:” ou “G:” – com direitos de leitura, escrita e exclusão.

§ 1° Os responsáveis pelas unidades poderão solicitar a criação de novas estruturas de diretórios na rede de computadores do Tribunal e definirão as permissões de acesso dos usuários sob sua responsabilidade.

§ 2° O limite de tamanho dos diretórios será fixado pela SETIN em norma interna, disponível na Intranet do Tribunal.

Art. 46. A rede possuirá um diretório temporário – denominado “H:” – com acesso permitido a todos os usuários, destinado à transferência de documentos.

Parágrafo único. O conteúdo deste diretório não terá cópia de segurança e será excluído diariamente.

Art. 47. A SETIN será responsável pelo controle e monitoramento das capacidades dos diretórios da rede de computadores do Tribunal e dos tipos de arquivos que poderão ser gravados nessas áreas.

Art. 48. Será vedada a cópia, em diretório da rede de computadores do Tribunal, dos seguintes tipos de arquivos:

I – imagens, músicas e filmes de qualquer formato;

II – programas não homologados ou não licenciados;

III – programas de conteúdo prejudicial à segurança do ambiente computacional;

IV – outros arquivos digitais cuja utilização não seja de interesse do Tribunal.

Parágrafo único. A SETIN poderá excluir dos diretórios da rede os arquivos que se enquadrem nas alíneas de I a IV deste artigo, sem prévio aviso e sem realizar cópia de segurança dos arquivos excluídos.

Art. 49. Será responsabilidade do usuário da rede de computadores do TST:

I – utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais;

II – primar pela eficiência na utilização dos recursos tecnológicos disponíveis, eliminando periodicamente os arquivos que não sejam necessários ou não façam parte do acervo de sua unidade;

III – não permitir acesso de terceiros à rede por meio de sua senha;

IV – notificar a SETIN, pelo endereço seguranca@tst.jus.br, quando tiver ciência da existência de arquivos na rede vedados, conforme o disposto no art. 37 deste Ato.

Art. 50. O acesso efetuado pela rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

## CAPÍTULO VIII

## DA UTILIZAÇÃO DE PROGRAMAS E APLICATIVOS

Art. 51. Este capítulo trata das diretrizes de homologação, instalação e utilização de programas e aplicativos de computador no âmbito do Tribunal.

Art. 52. A instalação e a utilização de programas de computador no Tribunal estão sujeitas aos seguintes requisitos:

I – existência de licenças de uso em quantidade suficiente;

II – homologação pelos técnicos da SETIN;

III – conformidade com a atividade da instituição e com a área de atuação das unidades;

IV – compatibilidade com os demais programas utilizados;

V – adequação aos recursos computacionais disponíveis; e

VI – obediência a planejamentos, cronogramas e prioridades existentes.

Art. 53. O equipamento de informática distribuído no Tribunal terá a instalação, pelos técnicos da SETIN, dos programas e aplicativos básicos homologados que atendam aos requisitos do artigo anterior.

Art. 54. A instalação de programas e aplicativos em equipamento de informática do Tribunal deverá ser realizada, exclusivamente, por técnicos da SETIN.

Art. 55. Será vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.

Art. 56. Caberá à SETIN manter o registro das licenças de uso de programas de terceiros utilizados pelo Tribunal.

Art. 57. A SETIN poderá autorizar a cessão de cópia de programa de computador adquirido ou contratado pelo Tribunal, em ambiente externo, nos termos da licença de uso.

Art. 58. A SETIN poderá realizar, para teste e avaliação, a instalação de programa ou aplicativo, com autorização do produtor, distribuidor ou revendedor, pelo prazo estipulado na autorização.

Art. 59. O usuário será responsabilizado pela instalação ou execução não autorizada de programa não homologado pela SETIN, considerando a possibilidade de dano às instalações de informática do Tribunal.

Art. 60. Será vedada a instalação e utilização de programas e aplicativos de computador que descaracterizem os propósitos da instituição e que possam prejudicar a segurança dos ativos de informação ou danificar o ambiente computacional do Tribunal.

Art. 61. A solicitação de instalação de programas e aplicativos deverá ser encaminhada à SETIN pelo Sistema de Solicitação de Serviços, acompanhada de justificativa.

Art. 62. A listagem dos programas e aplicativos homologados para a utilização no Tribunal deverá ser publicada na Intranet.

Art. 63. A SETIN deverá inventariar, sistematicamente, os programas e aplicativos instalados no Tribunal remotamente, sem prévia autorização do usuário.

Art. 64. A SETIN poderá remover, sem prévio aviso ao usuário e sem a realização de cópia de segurança, os programas e aplicativos que não cumprirem os requisitos do art. 52 deste Ato.

Art. 65. A atualização dos programas e aplicativos instalados no âmbito do Tribunal poderá ser realizada pela equipe técnica da SETIN remotamente, sem prévia autorização do usuário.

## CAPÍTULO IX

## DA UTILIZAÇÃO DE EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 66. A instalação de programas e aplicativos nos equipamentos portáteis do Tribunal observará os requisitos relacionados no art. 52 deste Ato.

Art. 67. Os microcomputadores portáteis pertencentes ao parque computacional do Tribunal deverão possuir a mesma proteção das estações de trabalho.

Art. 68. Será vedada a conexão de equipamento ou dispositivo móvel na Rede de Computadores do TST, sem a prévia verificação e autorização da equipe técnica da SETIN.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 69. Os dispositivos móveis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus antes de serem conectados a equipamento pertencente ao Tribunal.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 70. A solicitação de verificação de equipamento ou dispositivo móvel para autorização de conexão na rede de computadores do Tribunal deverá ser encaminhada à SETIN pelo Sistema de Solicitação de Serviços, acompanhada de justificativa.

Art. 71. O acesso efetuado pelos dispositivos móveis no ambiente tecnológico do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

## CAPÍTULO X

## DO CONTROLE, MONITORAMENTO E AUDITORIA DE RECURSOS TECNOLÓGICOS

Art. 72. A utilização de recursos tecnológicos bem como o acesso aos ativos de informação no Tribunal serão registrados e monitorados pela SETIN, com o intuito de detectar e evidenciar incidentes de segurança.

Parágrafo único. Não será realizado o monitoramento de serviço de telefonia móvel ou fixa.

Art. 73. A SETIN será responsável por realizar auditorias ordinárias e extraordinárias nos ativos de informação do Tribunal.

§ 1° Auditorias ordinárias serão realizadas periodicamente, com o objetivo de avaliação da conformidade técnica dos serviços, ferramentas e equipamentos em funcionamento no Tribunal.

§ 2° Auditorias extraordinárias serão requeridas por solicitação superior para apurar eventos que colocam em risco a segurança dos ativos de informação e as boas práticas de utilização do ambiente informatizado do Tribunal.

Art. 74. Estarão sujeitos à auditoria extraordinária os seguintes eventos de segurança:

I – Na estação de trabalho: alteração de arquivos e da configuração da estação de trabalho;

II – Nos dispositivos móveis: alteração de arquivos e da configuração do dispositivo, acessos ou manipulação de dados indevidos;

III – Nos sistemas informatizados e nos bancos de dados do Tribunal: acessos ou manipulação de dados indevidos;

IV – No correio eletrônico corporativo: envio e recebimento de mensagens eletrônicas indevidas;

V – No acesso à Intranet, à Internet ou outro meio de acesso externo à rede de computadores do Tribunal: acessos e manipulação de dados indevidos;

VI – Na rede de computadores do Tribunal: alteração de arquivos e da configuração dos servidores.

Art. 75. A solicitação de auditoria em incidente não previsto neste Ato será analisada e deliberada pelo Comitê Gestor de Segurança da Informação.

## CAPÍTULO XI

## DA ANÁLISE DOS RISCOS E DAS VULNERABILIDADES DO AMBIENTE COMPUTACIONAL

Art. 76. À SETIN caberá, periodicamente, a avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de suas ocorrências.

Art. 77. A SETIN manterá, instalado e atualizado, programa de detecção e proteção contra vírus e demais agentes nocivos à segurança dos ativos de informação no ambiente computacional do Tribunal.

Art. 78. Serão mantidos pela SETIN os planos de continuidade de negócios que visem a assegurar a integridade, a confidencialidade e a disponibilidade dos ativos de informação necessários para o cumprimento da missão institucional do Tribunal.

## CAPÍTULO XII

## DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 79. O usuário que efetuar qualquer acesso aos recursos computacionais do Tribunal que desrespeite este Ato será responsabilizado.

Art. 80. A SETIN poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso concedido ao usuário.

Art. 81. Caberá ao Comitê Gestor de Segurança da Informação, constituído pelo Ato TST.GP nº 493/2009, a revisão anual desta Política de Segurança da Informação.

Art 82. A inobservância das disposições deste Ato implicará responsabilidade administrativa na forma da lei.

Art. 83. O presente Ato entra em vigor a partir da data de sua publicação e revoga o ATO.GDGCA.GP.Nº 323/2006.

**Ministro JOÃO ORESTE DALAZEN**