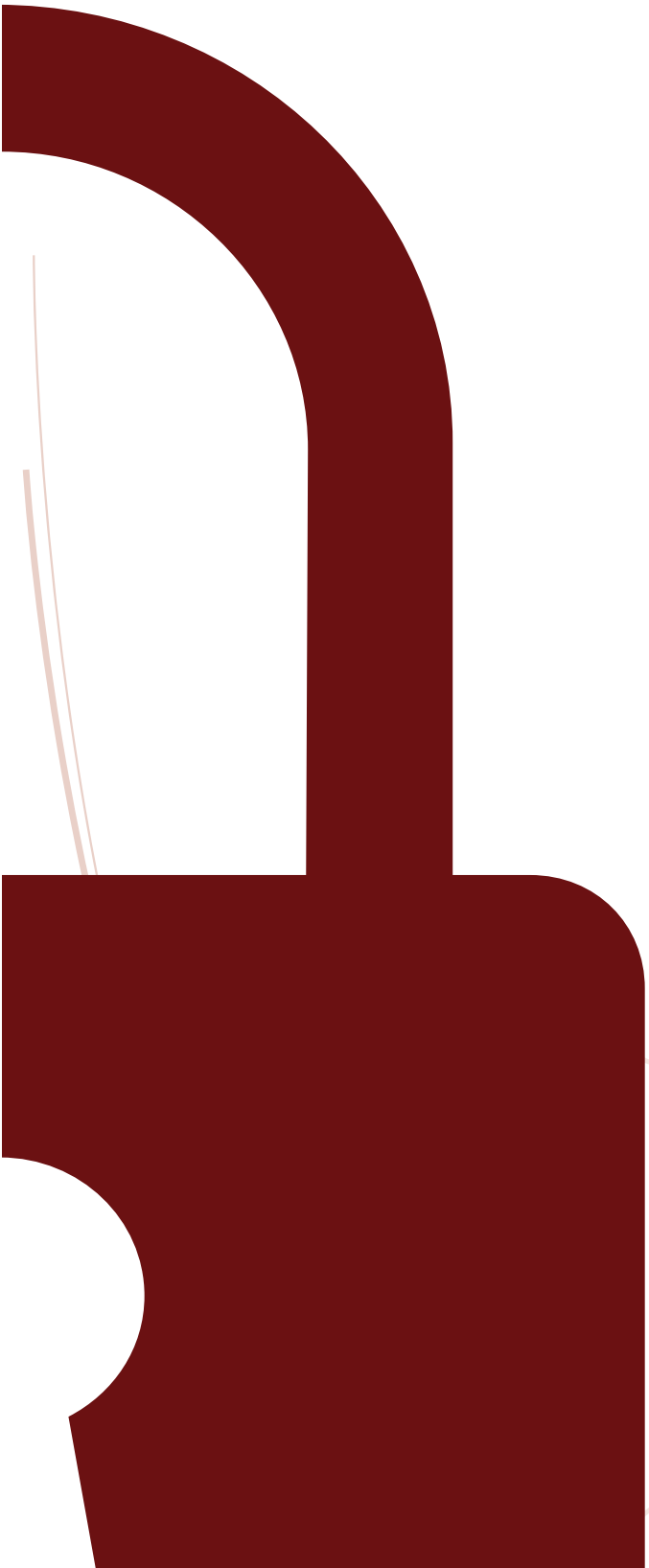
Superior Tribunal de Justiça

Secretaria de Controle Interno

CARTILHA

segurança da informação

Coordenadoria de Auditoria de Tecnologia da Informação



O que você faz para proteger as informações do STJ?

Você já ouviu falar no caso Snowden? O ex-técnico da CIA, Edward Snowden, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos. Ele revelou, em detalhes, alguns dos programas de vigilância que o país usa para espionar a população americana e de vários países da Europa e da América Latina, entre eles o Brasil. O governo americano é conhecido por ter uma segurança praticamente à prova de falhas. Nesse caso, no entanto, o fator humano foi o elo mais fraco, que levou à quebra da segurança e a um escândalo internacional.

No STJ, transitam todos os dias informações confidenciais que trariam um grande prejuízo à imagem do órgão e às pessoas envolvidas, caso fossem divulgadas. A Segurança da Informação é um processo, não um produto, e o nível de segurança geral é equivalente à segurança do elo mais fraco. Por isso, é importante conscientizar cada servidor do seu papel dentro da Segurança da Informação. De nada adianta garantir a segurança de sistemas informatizados, por exemplo, se o servidor falar abertamente sobre assuntos sigilosos em locais públicos.

Após a realização do levantamento de Segurança da Informação feito pela Coordenadoria de Auditoria de Tecnologia da Informação - CAUT, a Secretaria de Controle Interno constatou a necessidade de uma ação de conscientização sobre a Segurança da Informação. Como forma de contribuição para a missão do Tribunal da Cidadania, a Secretaria de Controle Interno, por meio da equipe da CAUT, elaborou esta cartilha de conscientização.

Desejamos que a leitura deste material seja proveitosa e que as orientações aqui repassadas façam parte do seu cotidiano.

Ângela Merce Teixeira Neves
Secretária de Controle Interno

A importância da informação na sociedade e na organização

Na sociedade atual, a informação assume uma importância cada vez maior, a ponto de se tornar o bem de maior valor para a maioria das organizações. A informação é o ingrediente básico do qual dependem os processos de decisão e de apoio. Assim, quanto maior a importância de determinada informação para a organização, maior é a necessidade de que essa informação se mantenha confiável, precisa e disponível para as pessoas autorizadas.

Em muitos casos, é importante que um número limitado de pessoas tenha acesso a essas informações, seja para evitar o vazamento de informações estratégicas da organização, seja para proteger a privacidade de pessoas.

Em um ambiente cada vez mais interconectado, no qual a informação assume papel cada vez mais relevante, cresce também a necessidade de proteção desse ativo essencial para os objetivos institucionais.

Como consequência do aumento no tráfego de informações, crescem também as **ameaças e vulnerabilidades** às quais a informação está exposta. Seja qual for sua forma de apresentação ou meio no qual está armazenada ou é transferida, é necessária a proteção adequada desse ativo.

Ameaças e Vulnerabilidades

De acordo com a ISO/IEC 27000:2014:

ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Pra que serve a Segurança da Informação

A Segurança da Informação é necessária para garantir a proteção das informações corporativas ou pessoais, assegurando que nenhuma informação seja alterada ou utilizada indevidamente. A Segurança da Informação é garantida por meio da preservação de alguns atributos básicos, também conhecidos como os **cinco pilares da Segurança da Informação**:

CONFIDENCIALIDADE

É a garantia de que somente pessoas autorizadas terão acesso à informação.

INTEGRIDADE

É a garantia de que a informação mantém as características originais estabelecidas por seu proprietário, ou seja, de que não foi modificada ou alterada de forma indevida.

DISPONIBILIDADE

É a garantia de que a informação estará pronta para o uso (por pessoas autorizadas) quando for necessária.

AUTENTICIDADE

É a garantia de que a informação vem da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser.

IRRETRATABILIDADE

Também chamada de **não-repúdio**. É a garantia de que a pessoa não negue ter assinado ou criado a informação.

CLASSIFICAÇÃO

Classificação das informações

Para proteger corretamente as informações, é necessário que exista uma forma de avaliar sua importância e de saber quais pessoas podem ter acesso ao seu conteúdo. O valor das informações produzidas e custodiadas pelo STJ é de grande importância não somente para os seus Ministros e servidores, mas também para todos os cidadãos. Dessa forma, é fundamental que a informação tenha o devido tratamento.

Existem várias formas de classificar a informação quanto ao seu nível de sigilo. Algumas são previstas em normas - como a NBR ISO/IEC 27002:2013 - ou manuais de boas práticas. O importante é que os níveis de sigilo sejam adaptados para a realidade de cada organização e amplamente divulgados, para que todos conheçam o significado de cada nível e saibam lidar com eles.

CONFIDENCIAL

A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais. É sempre restrita a um grupo específico de pessoas.

INTERNA

É uma informação que a organização não tem interesse em divulgar, mas que é importante para o público interno. Caso essa informação seja acessada indevidamente, podem ocorrer danos à imagem da Organização, mas não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por funcionários (ou servidores) e prestadores de serviços.

PÚBLICA

É uma informação com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional.

Podem ser citadas também as seguintes classificações de sigilo para as informações

SECRETA

São assuntos que requeiram alto grau de segurança e cujo teor ou características podem ser de conhecimento apenas de pessoas que estejam autorizadas a isso. São documentos considerados secretos os referentes a planos, programas e medidas governamentais e os assuntos extraídos de matéria ultrassecreta que necessitam de maior difusão, sem comprometer seu sigilo.

ULTRASSECRETA

Essa classificação é dada aos assuntos que requeiram excepcional grau de segurança e cujo teor ou características só devam ser do conhecimento de pessoas intimamente ligadas ao seu estudo ou manuseio. São normalmente assuntos ligados a temas como política governamental de alto nível e segredos de Estado como: negociações para alianças políticas e militares, planos de guerra, descobertas e experimentos científicos de valor excepcional etc.

Política de Segurança da Informação (PSI)

As políticas de segurança da informação definem os direitos e as responsabilidades de cada um em relação à Segurança da Informação.

Em geral, essas políticas são consolidadas em um documento geral, chamado simplesmente de **Política de Segurança da Informação - PSI**. Embora muitas vezes seja focada na área de Tecnologia da Informação, o ideal é que a **PSI** aborde todos os aspectos da Segurança da Informação e de maneira organizacional, mesmo aqueles que não estão diretamente envolvidos com recursos computacionais.

Esse documento geral deve ser focado nos requisitos de estratégia de negócio, regulamentações e legislação, além do ambiente de riscos e ameaças da segurança da informação, atuais e futuros.

A **PSI** deve conter declarações relativas às definições de Segurança da Informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação. Também deve conter a atribuição de responsabilidades gerais e específicas para o gerenciamento de segurança da informação e os processos de tratamento dos desvios e exceções.

O documento principal deve possuir uma linguagem simples e direta, sem entrar em detalhes técnicos. A **PSI** é um documento voltado para todos os colaboradores internos e partes externas relevantes e, como tal, deve ter uma linguagem acessível para que seja compreendida por todos.

A **PSI** pode ser apoiada por políticas específicas do tema, detalhadas de forma a considerar as necessidades de grupos específicos de interesse dentro da organização ou para cobrir determinados tópicos. São exemplos disso: controle de acesso, segurança física do ambiente, política de backup e senhas, identificação pessoal, entre outros.

PSI

Quem é responsável?

De acordo com a NBR ISO/IEC 27002:2013, a **PSI** deve ser definida pelo mais alto nível da organização e deve ser aprovada pela direção da organização.

Cada política de segurança da informação, ou seja, cada item principal da **PSI** deve ter um gestor responsável pelo seu desenvolvimento, análise crítica e avaliação periódica.

Quem deve ter acesso?

A **PSI** deve ser comunicada a todos os colaboradores da organização, ou seja, funcionários, dirigentes, prestadores de serviço, estagiários e até mesmo ao público externo, em alguns casos. Essa informação deve estar facilmente acessível a todos os usuários e constar em programas de conscientização e educação corporativos. Os desdobramentos da **PSI**, ou seja, o detalhamento de cada política também deve estar disponível de forma simples e rápida para todos os envolvidos em tal política.

Pode ser modificada?

A **PSI** não só pode como **deve** passar por um processovde revisão e modificação. O gestor de cada política deve fazer periodicamente uma análise crítica e avaliação de suas políticas. Essa análise deve incluir a avaliação de oportunidades para melhoria da política de segurança da informação da organização e para que ela se adeque às mudanças no ambiente organizacional, às circunstâncias do negócio, às condições legais ou ao ambiente de tecnologia.

Objetivos de segurança

Ao definir a **PSI**, os gestores devem pensar nos objetivos de segurança a serem atingidos. É comum ver organizações tentando classificar todas as suas informações com um alto grau de sigilo. No entanto, isso custa caro, e na maioria das vezes não é necessário. Saber adequar as políticas à realidade de cada organização é fundamental para o sucesso da implantação de uma **PSI**.

Ameaças, riscos e impactos

Além dos objetivos de segurança, é necessário conhecer os riscos e ameaças à segurança da informação. O que é mais importante para a organização: o sigilo das informações, sua disponibilidade ou a garantia de que nenhuma informação será perdida? Todos são pontos importantes, mas é necessária uma priorização para criar uma boa **PSI** e para auxiliar na criação de um Plano de Contingência.

O Plano de Contingência irá definir as ações tomadas para diminuir os riscos e o impacto das possíveis ameaças à Segurança da Informação. Políticas de backup e redundância ou mesmo treinamentos de prevenção e combate a incêndios são exemplos de Planos de Contingência.

Sanções e punições

Infelizmente, de nada adianta criar regras se as pessoas envolvidas não as seguirem. Dessa forma, a **PSI** também deve definir as sanções e punições a serem aplicadas para situações em que as políticas definidas sejam desrespeitadas.

Divulgação

Finalmente, uma vez que seja criada a **PSI**, é fundamental que ela seja amplamente divulgada entre os colaboradores internos da organização,e faça parte de programas de treinamento e de reciclagem constantes.

PAPÉIS

O papel de Ministros, servidores, estagiários e terceirizados no processo de Segurança da Informação.

Todos os dias trafegam milhares de informações no STJ, seja por seus corredores, seja através dos sistemas informatizados. Cada processo judicial ou administrativo representa um conjunto de informações, destinado a receptores específicos, sejam eles os próprios Ministros e servidores do STJ, sejam as partes envolvidas em cada processo. É essencial que essas informações consigam chegar a seus destinatários - e somente a eles.

É natural nos lembrarmos da Segurança da Informação apenas enquanto ela está nos computadores e sistemas informatizados. Assim, utilizamos senhas de acesso e antivírus, exigimos criptografia e outros controles. No entanto, a principal falha de segurança em qualquer sistema está fora dele: o ser humano.

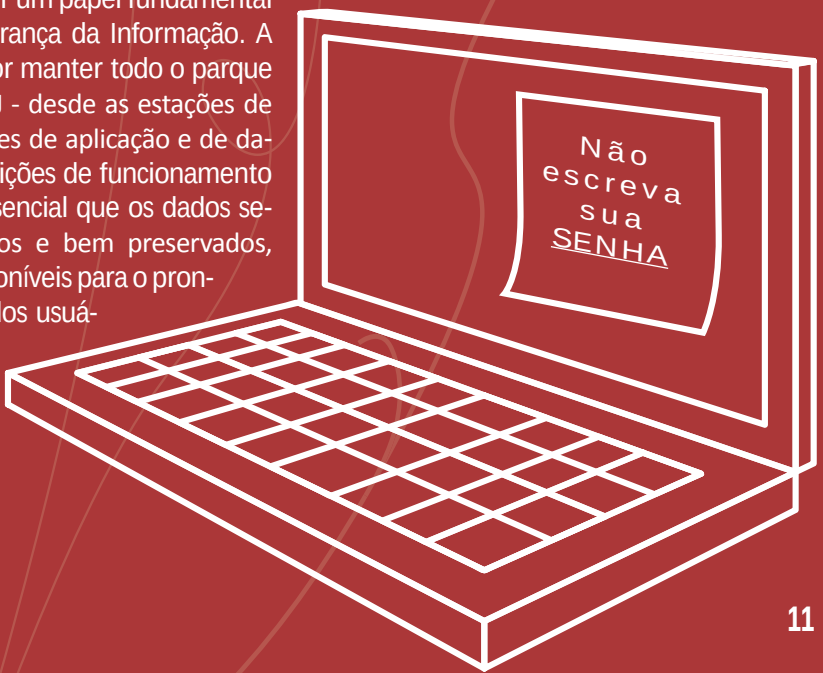
A forma mais fácil de conseguir qualquer informação sigilosa é através da chamada Engenharia Social, que nada mais é do que conseguir enganar alguém para ter acesso a informações privilegiadas. Seja ouvindo conversas alheias ou perguntando diretamente, pessoas mal intencionadas podem conseguir diversas informações importantes sem precisar sequer chegar perto de um computador.

Dessa forma, todos que frequentam o STJ - Ministros, servidores, estagiários ou terceirizados - devem ter consciência da importância do sigilo e da discrição em relação às informações classificadas. Não adianta ter um ambiente tecnológico seguro se as informações são impressas e deixadas sobre a mesa, em um local onde qualquer um pode ter acesso. Da mesma forma, não adianta ter senha no computador se o usuário tem o costume de sair de sua mesa e deixar o computador desbloqueado. Ou ainda, não adianta ter todo o cuidado com informações sigilosas escritas, mas comentá-las de forma aberta e descuidada em um ambiente público, como o restaurante.

Assim, é importante não só que apenas as pessoas autorizadas para cada nível de sigilo tenham acesso àquelas informações, mas também que tais pessoas sejam cuidadosas ao lidar com essas informações, evitando que elas sejam transmitidas - seja de forma voluntária ou involuntária - para pessoas que não estão autorizadas.

O papel da Tecnologia da Informação no processo de Segurança da Informação.

Com o processo judicial eletrônico e a automatização cada vez maior dos processos administrativos do Tribunal, a área de Tecnologia da Informação passa a ter um papel fundamental no processo de Segurança da Informação. A área é responsável por manter todo o parque computacional do STJ - desde as estações de trabalho aos servidores de aplicação e de dados - em plenas condições de funcionamento e de segurança. É essencial que os dados sejam mantidos íntegros e bem preservados, além de estarem disponíveis para o pronto acesso por parte dos usuários autorizados.



DICAS

10 dicas
sobre Segurança da Informação

Conheça a política de segurança
Procure estar ciente da política de segurança do STJ e dos serviços que você utiliza (como Webmail e redes sociais).

Confidencialidade e Privacidade
Fique atento à política de confidencialidade do STJ e seja cuidadoso ao divulgar informações profissionais, principalmente em blogs e redes sociais.

Não repasse informações confidenciais
Não efetue gravação ou cópia, nem se aproprie ou repasse documentação confidencial a que tiver acesso.

Cuidados depois da impressão ou cópia dos arquivos
Não basta que a informação esteja protegida na rede em meio digital, é preciso também pensar na segurança depois que imprimimos ou copiamos os arquivos. Documentos impressos sobre a mesa ou em gavetas sem tranca são possíveis fontes de vazamento de informações sigilosas.

Bloqueio da máquina
Bloqueie sua máquina em caso de ausência e a desligue ao final do expediente.

Cuidado com mensagens oriundas da internet

Mensagens recebidas da Internet que não são de interesse do órgão não devem ser repassadas através do correio eletrônico corporativo. A mesma orientação vale para mensagens sobre vírus ou ameaças de segurança que aconselham o repasse das mensagens para outras pessoas. Nesses casos, o usuário deve eliminar a mensagem e jamais repassar internamente na empresa.

Responsabilidade pelas informações

Você é responsável pelas informações armazenadas nos equipamentos de seu uso exclusivo.

Uso do correio eletrônico

A utilização do correio eletrônico deve ser restrita às atividades de interesse da empresa e as mensagens transmitidas pelo correio eletrônico não devem conter dados e informações confidenciais ou vitais do órgão, a não ser que adequadamente protegidas por senha ou criptografia e em conformidade com as políticas de segurança.

Cuidado com suas senhas

Mantenha suas senhas em sigilo absoluto, não revelando a outras pessoas nem as anotando.

Encontrou algo de errado? Comunique ao responsável

Você deve informar ao responsável quando se deparar com algo que possa comprometer a segurança da informação no Tribunal.

Normas e publicações relacionadas

- **Família de Normas ISO/IEC 27000**
  Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações.
- **Boas Práticas em Segurança da Informação - TCU - 4ª Edição - 2012**
  Publicação do Tribunal de Contas da União com o intuito de despertar a atenção para os aspectos da segurança da informação nas instituições governamentais.
- **Decreto n.º 3.505, de 13.06.2000**
  Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- **Cartilha de Segurança para Internet - cert.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  Contém recomendações e dicas sobre como aumentar a segurança ao navegar na internet.
- **Portaria STJ n. 898 de 31 de dezembro de 2009**
  Dispõe sobre a implantação do Programa de Gestão Documental - AGILIS.
- **Portaria STJ n. 898 de 31 de dezembro de 2009 - Anexo 1**
  Dispõe sobre as rotinas e procedimentos de criação, captura e digitalização do Programa de Gestão Documental - AGILIS.
- **Plano de classificação e tabelas de temporalidade dos documentos da Administração Judiciária do Superior Tribunal de Justiça - STJ**
  Define o Plano de Classificação e Tabela de Temporalidade dos Documentos da Administração Judiciária do STJ.
- **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.
- **Resolução STJ n. 8 de 13 de novembro de 2009**
  Institui o Código de Conduta do Superior Tribunal de Justiça.
- **Resolução STJ n. 20 de 9 de agosto de 2012**
  Dispõe sobre a certificação digital no Superior Tribunal de Justiça e dá outras providências.
- **Portaria STJ n. 25 de 1º de fevereiro de 2008**
  Institui a política de utilização dos recursos de tecnologia da informação no âmbito do Superior Tribunal de Justiça.

EQUIPE

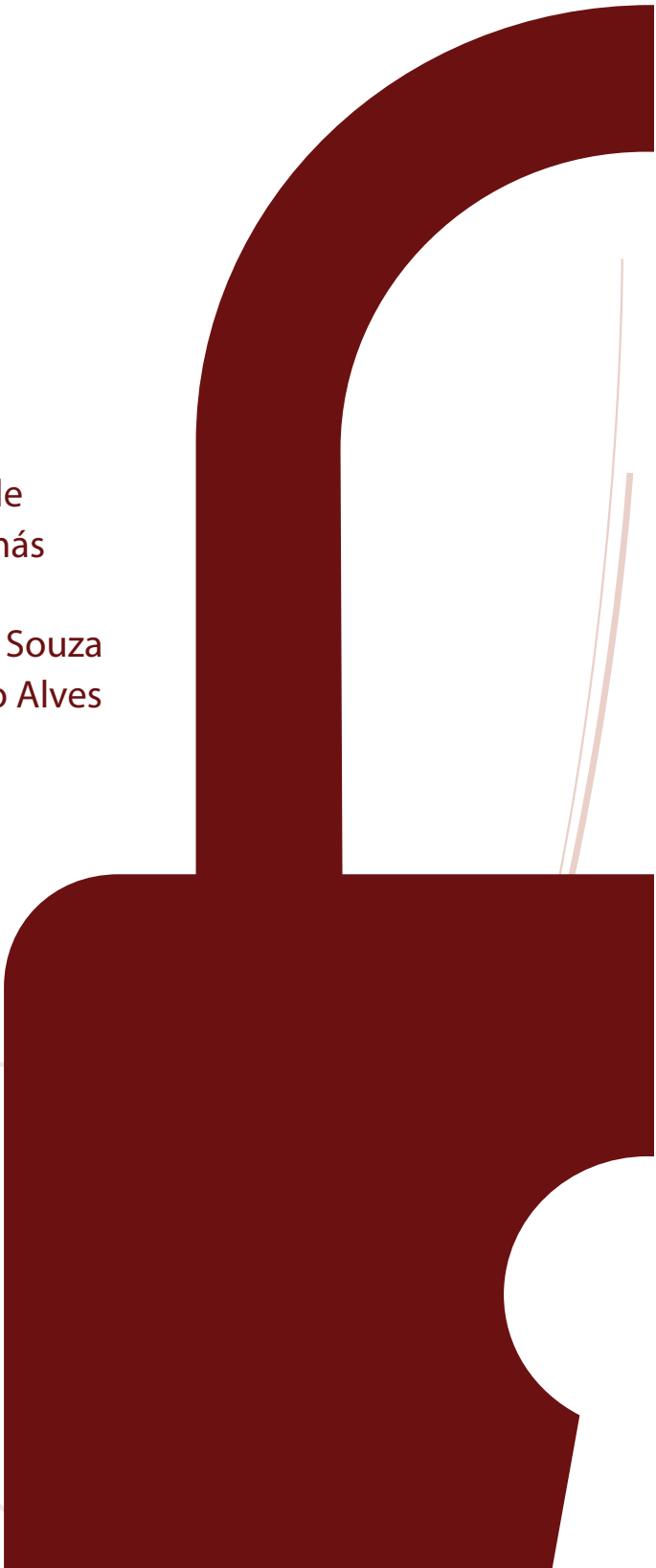
Wadson Sampaio Pereira
Gustavo de Moura Rocha
Vitor Dutra Freire
João Augusto Mendes Vale
Eliane Maria Cordeiro Tomás
Leonardo Ramos Paz
Paulo Henrique Rocha de Souza
Sérgio Giovane Canavarro Alves
Camila Melo de Carvalho
Michel Viana Oliveira

COORDENAÇÃO

Silvia Caldas Ferreira

DESIGN

Vitor Dutra Freire



Um programa de conscientização sobre segurança da informação tem como objetivo principal influenciar servidores e colaboradores a mudarem seus hábitos, bem como criar a consciência de que todos são corresponsáveis pela Segurança da Informação. Esse processo de conscientização deve ser contínuo, para manter os usuários alertas e para prepará-los para os novos riscos e ameaças que surgem a cada dia.

Além dos aspectos gerais de Segurança da Informação, cada área deve ter um treinamento adequado a sua realidade. As políticas podem ser gerais, aplicadas a todos, ou específicas, aplicadas nas situações em que é necessária a existência de políticas e treinamentos específicos para determinados cargos ou grupos distintos dentro da organização, como, por exemplo, os gestores, o pessoal da tecnologia, os usuários de microcomputadores, o pessoal das áreas não técnicas, os assistentes administrativos, recepcionistas e o pessoal da segurança física.

Um órgão que leva a Segurança da Informação a sério mantém os riscos e ameaças sob controle e não coloca em jogo a sua imagem organizacional. Com isso, toda a instituição ganha e mantém seu objetivo maior: prestar um serviço de qualidade para o cidadão brasileiro.

STJ
SUPERIOR TRIBUNAL DE JUSTIÇA

Secretaria de Controle Interno
Coordenadoria de Auditoria de Tecnologia da Informação