Casoteca ADM

# Não é só trocar a senha

## Segurança Cibernética no Tribunal Superior

Beatriz Teles Fernandez
Renato Solimar Alves
Gabriel Marinho Godinho
Carlos Eduardo Miranda Zottmann
Rafael Rabelo Nunes
Nicole Alonso Santos de Sousa
Luiz Henrique Lima Rodrigues

# Não é só trocar a senha: Segurança Cibernética no Tribunal Superior

Casoteca ADM

This book is for sale at http://leanpub.com/segurancacibernetica

This version was published on 2024-01-03

# Contents

**Não é só trocar a senha: Segurança Cibernética no Tribunal Superior** . . . . . **1**
Resumo . . . . . 1
Abstract . . . . . 2
Caminhos Jurídicos: A Jornada de Clarice no Tribunal . . 2
Além dos Muros: A Invasão Cibernética e o Vazamento de Dados . . . . . 4
O impacto foi grande! E agora? . . . . . 6
Segurança da informação: Um panorama geral . . . . . 8
Estou seguro? O Que Devo Saber? . . . . . 10
Departamentos do Tribunal e a Segurança de seus Processos de Negócio . . . . . 16
Segurança e Eficiência Operacional: uma relação inversamente proporcional . . . . . 17
Um olhar para fora: Comparando com Outras Organizações 19
Fortalecendo a Segurança Cibernética . . . . . 20
Perguntas para o debate . . . . . 22
Nota dos autores . . . . . 23
Galeria . . . . . 23
Referências . . . . . 26
Sobre os autores . . . . . 29

# Não é só trocar a senha: Segurança Cibernética no Tribunal Superior

Autores:

- Beatriz Teles Fernandez
- Gabriel Marinho Godinho
- Renato Solimar Alves
- Carlos Eduardo Miranda Zottmann
- Rafael Rabelo Nunes

## Resumo

Recentemente, o Tribunal Superior foi alvo de um ataque hacker, demandando uma urgente revisão e fortalecimento de suas medidas de segurança cibernética. Clarice, estagiária do Escritório de Gestão de Processos Organizacionais, assumiu a responsabilidade de conduzir uma pesquisa abrangente sobre segurança cibernética e apresentar um relatório com propostas de solução para mitigar os riscos enfrentados para subsidiar decisões estratégicas de re-organização do Tribunal. Este cenário proporciona uma oportunidade para discutir os fundamentos da segurança da informação, explorar estratégias para minimizar os riscos cibernéticos sem prejudicar a produtividade das organizações e examinar os desafios enfrentados pela alta gestão ao implementar controles de segurança em processos cruciais de negócios e gestão de riscos, convidando

o leitor a refletir sobre as lacunas que podem existir entre as práticas recomendadas e as efetivamente adotadas no âmbito da segurança cibernética. Ao contextualizar a situação nos Tribunais Superiores brasileiros, busca-se não apenas destacar a importância dessa discussão, mas também sensibilizar para a complexa interação entre segurança cibernética, eficiência operacional e cultura organizacional.

**Palavras-chave**: Segurança Cibernética, Tribunal de Justiça, Ataques Hacker, Gestão de Processos, Gestão de Riscos.

# Abstract

Recently, the Supreme Court has been the target of a hacker attack, demanding an urgent review and strengthening of its cybersecurity measures. Clarice, an intern at the Organizational Process Management Office, has taken on the responsibility of conducting thorough research on cybersecurity and presenting a report with proposed solutions to mitigate the risks faced in order to support strategic decisions to reorganize the Court. This scenario provides an opportunity to discuss the fundamentals of information security, explore strategies to minimize cyber risks without compromising organizational productivity, and examine the challenges faced by senior management in implementing security controls in critical business processes and risk management. This case invites the reader to reflect on the gaps that may exist between recommended practices and those actually adopted in the field of cybersecurity. By contextualizing the situation in Brazilian Supreme Courts, the aim is not only to underscore the importance of this discussion but also to raise awareness of the complex interaction between cybersecurity, operational efficiency, and organizational culture.

***Keywords:*** Cybersecurity, Judiciary, Hacker Attacks, Process Management, Risk Management.

# Caminhos Jurídicos: A Jornada de Clarice no Tribunal

Estudante de administração, em uma das aulas de Gestão de Processos, Clarice se interessou pela temática de Processos de Negócio, em especial, pela relevância que o controle da qualidade por processos de trabalho pode ter na realidade de uma organização. Como ainda não havia tido sua primeira experiência de estágio, buscou algum no qual pudesse desenvolver suas habilidades nessa área ou área correlata. Nessa procura, ela encontrou uma oportunidade inusitada: estagiar no Escritório de Gestão de Processos Organizacionais de um dos 5 Tribunais Superiores do Brasil (BRASIL, 1988), auxiliando no mapeamento e aprimoramento dos fluxos de processos de negócio do Órgão.

Ao entrar no Tribunal, Clarice teve suas expectativas amplamente superadas ao perceber as inovações tecnológicas que permeavam o ambiente. Era um verdadeiro vislumbre do futuro do sistema judiciário em rumo à sua Transformação Digital. Entre as novidades, ela observou a adoção de videochamadas para a realização de audiências, o que, na sua percepção, tornava a justiça mais acessível e ágil.

Além disso, o processo eletrônico, com todas as suas fases digitalizadas, desde o peticionamento até a finalização do processo, indicava uma mudança significativa na forma como a burocracia era enfrentada. E, para completar, o atendimento remoto por meio do "balcão virtual" mostrava que o Tribunal estava verdadeiramente abraçando a transformação digital para melhor servir a população.

Clarice estava animada para mergulhar nesse cenário de inovação enquanto auxiliava no mapeamento dos fluxos de processos de negócio. Seu estágio prometia ser uma jornada emocionante e repleta de aprendizado no coração do sistema judicial brasileiro.

Nos seus primeiros dias de estágio, a supervisora de Clarice realizou

um *onboarding*, no qual apresentou alguns documentos sobre a organização, dentre eles, o organograma do Tribunal Superior, o qual evidenciava todas as principais áreas e departamentos. Além do organograma, foi apresentada a ela a Cadeia de Valor, que evidenciava os principais macroprocessos realizados para atingir os objetivos e resultados da organização.

A partir da revisão dos materiais repassados por sua supervisora, Clarice pôde constatar algumas características do Tribunal, dentre elas: os juízes que atuam no Tribunal são chamados de ministros e todos eles são nomeados pelo presidente, mediante a aprovação prévia do Senado Federal. Além disso, os casos que ali são julgados ou começam diretamente no Tribunal ou revisam decisões dos tribunais estaduais e regionais federais (TRFs), ou seja, julgam recursos finais e importantes em processos judiciais.

Além disso, Clarice teve algumas dúvidas relacionadas à Cadeia de Valor do Tribunal referentes a quais seriam os macroprocessos de negócio que se destacam como finalísticos, uma vez que a Cadeia de Valor engloba muitos macroprocessos, tais como: o recebimento e distribuição de processos, análise e relatoria de processos, produção de decisão, julgamento, processamento judicial e execução de atos cartorários e o cumprimento de despachos e decisões.

A partir disso, ela decidiu agendar uma reunião para saná-las com sua supervisora, Fernanda, que lhe explicou que os macroprocessos relacionados à elaboração de despachos e de decisões são considerados como sendo os finalísticos para a organização, porque são executados diretamente pelos magistrados.

A partir dessa conversa com Fernanda, Clarice entendeu um pouco mais sobre a estrutura do Tribunal e dos macroprocessos de negócio que irá trabalhar ao longo do seu estágio.

# Além dos Muros: A Invasão Cibernética e o Vazamento de Dados

Em meio a esse mundo de informações novas e expectativas, um acontecimento abala o andamento do tribunal: um ataque cibernético a um dos sistemas utilizados pelo Tribunal. Tratava-se do sistema utilizado para a comunicação entre o tribunal e os jurisdicionados (advogados e partes do processo), contendo algumas ferramentas como pesquisa sobre consulta processual e disponibilização de informações gerais, como acesso ao acervo e dúvidas frequentes. Além disso, dentro do próprio órgão, o mesmo sistema era usado como ferramenta pelos colaboradores para movimentação dos processos, ou seja, a prestação jurisdicional passava por esse sistema.

Quando o ataque aconteceu, os colaboradores não sabiam muito bem o que estava acontecendo, pois o sistema apenas se apresentava como indisponível. Porém, à medida que o tempo foi passando e a situação não se normalizou, rumores sobre o ataque começaram a se espalhar, e um ar de desconfiança e medo instaurou-se, pois, para além do estresse de não conseguir concluir seus trabalhos, existia uma incerteza do que seria do sistema agora.

Posteriormente, verificou-se que o sistema apresentava suas limitações e vulnerabilidades, e foi por meio de uma delas que o atacante conseguiu infiltrar-se nele, ganhando acesso a informações confidenciais[1].

No entanto, ao invés de se apropriar das informações diretamente, o invasor implantou um tipo específico de ataque conhecido como '*ransomware*'. Esse tipo de ataque é caracterizado pelo uso de um malware, que criptografa todos os dados nos computadores e servidores comprometidos.

Posteriormente, o atacante exigiu um resgate em troca da chave de descriptografia necessária para recuperar as informações. É

importante observar que, segundo a legislação brasileira, não há respaldo legal para o pagamento de resgates em casos de ataques desse tipo.

Isso ocasionou uma instabilidade no sistema, fazendo com que ele ficasse fora do ar por um certo tempo, o que atrasou os processos e instaurou uma insegurança geral no tribunal.Em meio a essa situação, Clarice se viu perdida em seu primeiro grande problema no tribunal. Sem saber como proceder, ela recorreu à internet. Ocorreram 103,16 bilhões de tentativas de ataques cibernéticos em 2022, esse foi o dado levantado pela *FortiGuard Labs*, que Clarice encontrou enquanto pesquisava sobre segurança da informação e ataques cibernéticos. Clarice também teve seu trabalho afetado por um desses ataques, uma vez que utiliza o sistema invadido. Agora tanto ela quanto o tribunal vão ter que encarar essa nova realidade e tentar resolver essa situação, minimizando as consequências e repensando a segurança da informação dentro do tribunal para que a mesma situação não se repita.

## O impacto foi grande! E agora?

No Escritório de Gestão de Processos Organizacionais do Tribunal Superior, a rotina deu lugar a um turbilhão de caos e preocupação após o ataque hacker devastador... As consequências foram assustadoras e imediatamente visíveis em diversas frentes. Os sistemas de segurança foram insuficientes em suas funções, deixando expostas informações cruciais. Uma série de incidentes surgiu em cascata, abalando a essência da justiça que o Tribunal representava.

Miguel, o chefe do Escritório de Gestão de Processos Organizacionais, e sua equipe rapidamente perceberam as consequências do ataque. As informações necessárias para o processo decisório na cadeia de fornecimento de dados foram alteradas, gerando confusão e incerteza entre os magistrados.

Alguns dos processos sigilosos também foram expostos, causando indignação e preocupação generalizada. Além disso, em investigação no incidente, verificou-se que os hackers tiveram acesso antecipado a determinações e decisões em curso, mesmo sem modificá-las, colocando em xeque a credibilidade do sistema judicial. Decisões que poderiam moldar o futuro de casos importantes estavam comprometidas.

A prestação jurisdicional foi interrompida, com os sistemas paralisados pelos invasores cibernéticos. O Tribunal se encontrava vulnerável, e todos os esforços do Escritório de Gestão de Processos Organizacionais pareciam insuficientes diante dessa ameaça virtual.

O ataque hacker desencadeou uma corrida contra o tempo para restaurar os sistemas e a própria integridade da imagem do Tribunal. Em tempo, medidas paliativas foram implementadas para conter os impactos imediatos. No entanto, os danos deixados por esse ato eram profundos, e a jornada rumo à recuperação completa estava apenas começando. Agora, além da recuperação, o foco estava em aprimorar a segurança e os processos, indo além das soluções emergenciais já implementadas.

Os esforços para reverter os impactos desse ataque sem precedentes estava apenas começando, e cada membro do Tribunal sabia que seu empenho e dedicação seriam cruciais para proteger a integridade do Tribunal e garantir que a justiça prevalecesse.

Não obstante, Clarice estava insegura e ansiosa, sem saber o que poderia fazer diante do cenário que lhe foi apresentado. Diante disso, solicitou uma reunião de alinhamento com sua supervisora para entender qual seria a melhor forma de ajudar o Escritório a implementar soluções aos problemas emergentes.

**Clarice**: Fernanda, estou um pouco apreensiva com essa reunião. A situação após o ataque hacker deixou todos nós preocupados.

**Fernanda (supervisora)**: O ataque foi realmente preocupante, mas é por isso que precisamos nos fortalecer ainda mais. Quero que

você se concentre em uma tarefa importante... Como estagiária do Escritório de Gestão de Processos Organizacionais, gostaria que você realizasse uma pesquisa juntamente com o Rodrigo, um dos gerentes do Escritório de Gestão de Processos, para levantar possíveis diretrizes focadas no aumento da segurança dos fluxos de processo de negócio do Tribunal. Para isso, consultem também a equipe de tecnologia, que pode auxiliar a compreender melhor os desafios.

**Clarice**: Vou me empenhar para realizar essa pesquisa. Espero que ela possa contribuir de alguma forma com as ações futuras para o aprimoramento dos processos.

**Fernanda**: Exatamente, Clarice. Confio plenamente em sua capacidade e sei que sob a tutoria de Rodrigo, vocês dois trarão ideias valiosas com potencial para aprimorar nossos processos. Pesquise as melhores práticas em segurança cibernética, explore tecnologias, *frameworks* e, se necessário, consulte o pessoal da Secretaria de TI.

Dados esses direcionamentos, Clarice ficou empolgada com a demanda que lhe foi atribuída e com a oportunidade de gerar um impacto tão relevante no seu primeiro estágio juntamente com um dos gerentes. Com isso, iniciou-se uma pesquisa de alternativas para tentar descobrir como a organização pode se estruturar melhor para enfrentar esse tipo de risco cibernético, a partir de uma pesquisa que explora tanto como criar uma estratégia de prevenção quanto como aumentar a segurança do fluxo de processos do tribunal

## Segurança da informação: Um panorama geral

Para a concretizar a demanda que lhe foi passada, Rodrigo delimitou as etapas que os dois percorreriam para fazer a pesquisa, Figura 1.

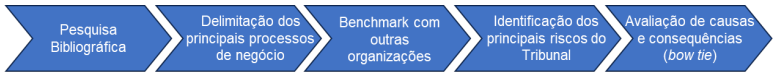


**Figure 1. Etapas da pesquisa de Clarice. Fonte: Adaptado de Alves, Renato S.; Georg, Marcus A. C.; Nunes, Rafael R., 2022.**

Na primeira etapa, "Pesquisa Bibliográfica", Clarice ficou responsável por identificar alguns tópicos relevantes para prevenir futuros ataques hackers no Tribunal. Conforme identificava esses temas, Clarice os registrava em um relatório, para que posteriormente fosse apresentado à Fernanda, sua supervisora, e Miguel, chefe do Escritório, consolidando os resultados das etapas delimitadas para a pesquisa.

Inspirada no seu trabalho na área pública, ela decidiu começar pelo o que está dito na lei, mais especificamente o que a LGPD, Lei Geral da Proteção de Dados, diz sobre a segurança da informação. Contudo, após analisar a lei, ela descobriu que não existe um método específico recomendando, a lei apenas cita que devem existir proteções adequadas - e isso, para a privacidade de dados - que se mostrou um outro universo.

Já Rodrigo realizou uma pesquisa sobre a parte de controles de segurança. Entre os tópicos encontrados, destacam-se os *frameworks* e publicações que sugerem os controles de segurança necessários para proteção à, por exemplo, ataques hackers:

**Controles de segurança e privacidade para sistemas de informação e organizações federais (NIST SP, 2020)**: Nessa publicação, Rodrigo identificou uma série de informações cruciais para aprimorar a segurança dos fluxos de processo de negócio do Tribunal Superior. A publicação estabelece controles específicos que podem ser implementados em qualquer organização ou sistema que lide com o processamento, armazenamento ou transmissão de informações. Esses controles visam reforçar a segurança cibernética e a privacidade, protegendo a instituição contra ameaças potenciais.

Rodrigo também percebeu que a publicação sugere a importância

de melhorar a comunicação entre as organizações, fornecendo um léxico comum para facilitar a discussão de conceitos de segurança, privacidade e gerenciamento de riscos. Isso possibilita que as equipes envolvidas na prevenção de riscos tenham uma compreensão unificada dos termos e objetivos, aprimorando assim a colaboração e eficácia das estratégias implementadas.

A publicação também descreve alguns dos conceitos fundamentais associados aos controles de segurança e privacidade, oferecendo uma visão abrangente dos princípios e fundamentos que guiam a implementação desses mecanismos de proteção. Um dos conceitos-chave que ela depreendeu foi o de 'Controles de Segurança'. Esses controles referem-se a práticas específicas que uma organização pode implementar para mitigar riscos de segurança cibernética e proteger seus sistemas e informações contra ameaças. Eles abrangem uma ampla gama de medidas, desde procedimentos e políticas de segurança até tecnologias e práticas operacionais.

Além disso, o catálogo consolidado de controles de segurança e privacidade presente na publicação é uma ferramenta valiosa para as organizações, fornecendo uma lista completa de controles específicos, cada um com uma seção de discussão que explica a finalidade de sua aplicação e oferece informações úteis sobre como implementá-los e avaliá-los adequadamente.

## Estou seguro? O Que Devo Saber?

Ao apresentar suas descobertas para Clarice, Rodrigo destacou que a publicação apresenta uma lista de controles relacionados, evidenciando os inter-relacionamentos e dependências entre os diferentes controles. Essa compreensão abrangente pode auxiliar o Escritório de Gestão de Processos Organizacionais a recomendar uma abordagem integrada e sinérgica na implementação dessas medidas de segurança.

**Cybersecurity Framework (tradução livre: Estrutura de segurança cibernética) do NIST V 1.1**: Consiste no framework que apresenta padrões, diretrizes e práticas do setor de uma maneira que permite a comunicação das atividades e dos resultados de segurança cibernética em toda a organização, desde o nível executivo até o nível de implementação/operações (NIST CSF, 2018). Ao ler a lista, Clarice pôde identificar cerca de 5 funções, 22 categorias, 98 subcategorias e aproximadamente 1200 controles de segurança, descritas no *framework*, Figura 2 (NIST, 2022, *apud* Alves, Renato S.; Georg, Marcus A. C.; Nunes, Rafael R., 2022).


**Figure 2. 5 funções do framework NIST. Fonte: (NIST, 2018)**

Clarice entendeu que, quando consideradas em conjunto, essas funções oferecem uma visão estratégica de alto nível do ciclo de

vida do gerenciamento de riscos de segurança cibernética de uma organização (NIST CSF, 2018). Em seguida, o *Framework Core* identifica as principais categorias e subcategorias subjacentes - que são resultados específicos - para cada função e as associa a exemplos de referências informativas, como normas, diretrizes e práticas existentes para cada subcategoria.

**Framework de segurança cibernética CIS Controls (CIS, 2021):** Dos *frameworks* e publicações estudados e apresentados por Rodrigo, Clarice considerou esse *framework* como sendo o mais didático e promissor, visto que foi construído a partir da simplificação das estruturas NISTs (NIST SP, 2020 e NIST CSF, 2018). Ela identificou no *White Paper* publicado por McClain & Sagerand (2018) que os 18 controles evidenciados nesse *framework* visam atender às necessidades das infraestruturas críticas da organização com a melhor relação entre risco e benefício. Isso é baseado no Princípio de Pareto, que diz que 20% das causas são responsáveis por cerca de 80% dos efeitos. Portanto, cerca de 20% dos controles do NIST podem proporcionar cerca de 80% de melhoria na segurança cibernética.

Clarice percebeu que a implementação dos controles do CIS CSC segue uma abordagem estruturada e progressiva. O processo começa com o grupo IG1, que é considerado obrigatório para todas as organizações, independentemente de seus recursos disponíveis. Essa primeira etapa é essencial para estabelecer uma base sólida de segurança, mesmo para organizações com recursos limitados.

Em seguida, o framework aborda o grupo IG2, que leva em conta organizações com recursos moderados. Nessa fase, são adicionados controles e medidas de segurança adicionais para enfrentar ameaças mais complexas e mitigar riscos em um nível intermediário.

Por fim, o grupo IG3 é destinado a organizações com exposição a alto risco, como é o caso do Tribunal Superior. Em conjunto, eles perceberam que terão de ser implementados controles avançados

e estratégias de segurança cibernética mais sofisticadas para combater ameaças extremamente sérias e proteger a organização contra ataques de alta complexidade (Figura 3).

| Grupos de Controles CIS CSC | IG1 | IG2 | IG3 |
|---|---|---|---|
| 1- Inventário e Controle de Dispositivos de *Hardware* | 2 | 4 | 5 |
| 2- Inventário e Controle de Ativos de *Software* | 3 | 6 | 7 |
| 3- Proteção de Dados | 6 | 12 | 14 |
| 4- Configuração Segura dos Softwares e Ativos Empresariais | 7 | 11 | 12 |
| 5- Grenciamento de Contas | 4 | 6 | 6 |
| 6- Gerenciamento do Controle de Acesso | 5 | 7 | 8 |
| 7- Gerenciamento Contínuo de Vulnerabilidades | 4 | 7 | 7 |
| 8- Gerenciamento dos Logs de Auditoria | 3 | 11 | 12 |
| 9- Proteção de *e-mails* e Navegadores WEB | 2 | 6 | 7 |
| 10- Proteção contra aplicações maliciosas | 3 | 7 | 7 |
| 11- Recuperação de Dados | 4 | 5 | 5 |
| 12- Gerenciamento da Infraestrutura de Rede | 1 | 7 | 8 |
| 13- Defesa e monitoramento da Rede | 0 | 6 | 11 |
| 14- Treinamento de Conscientização e Habilidades de Segurança | 8 | 9 | 9 |
| 15- Gerenciamento de Provedor de Serviços | 1 | 4 | 7 |
| 16- Segurança de Softwares e Aplicativos | 0 | 11 | 14 |
| 17- Gerenciamento de Resposta a Incidentes | 3 | 8 | 9 |
| 18- Teste de Penetração | 0 | 3 | 5 |

**Figure 3. Grupos de controle do CIS CSC e o número de sub controles. Fonte:(Lima, et al., 2022)**

Clarice percebeu que o *framework* oferece uma abordagem estratégica e bem estruturada para fortalecer a segurança cibernética do Tribunal. A divisão em três grupos - IG1, IG2 e IG3 - permite que a implementação dos controles seja adaptada às particularidades e recursos da instituição, tornando a abordagem mais flexível e acessível.

Identificadas algumas das publicações e *frameworks* para implantar possíveis controles de segurança no Tribunal Superior, Clarice percebe a necessidade de identificar os processos de negócio que devem ser priorizados para implementar os controles, visto que são vários os definidos pelos materiais estudados.

Diante disso, Rodrigo também identificou o 'Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário – PGCRC-PJ', Portaria CNJ n. 162 de 10 de junho de 2021, que estabelece os procedimentos responsivos a serem realizados no pré e pós a ocorrência de uma crise cibernética de média / longa duração. Nesse documento, ele pôde perceber que é necessário identificar as atividades primordiais para a manutenção da atividade finalística da organização, identificar os ativos que sustentam essas atividades e avaliar continuamente os riscos a que elas estão expostas e que essas são as ações previstas para a prevenção do risco da crise cibernética (Conselho Nacional de Justiça, 2021a, pp. 15-16).

De posse dessas informações, Clarice lembra da conversa que teve com sua supervisora no início do estágio, na qual ela tira dúvidas sobre a Cadeia de Valor. Nessa conversa, Fernanda explica que os processos de negócio, 'elaboração de despachos e de decisões', são os considerados finalísticos para a organização, já que são executados diretamente pelos magistrados. Dessa forma, Clarice conclui que serão esses os priorizados em seu relatório.

Após a priorização dos processos de negócio, respectivos ao Tribunal Superior, Clarice busca entender, analisando os impactos do incidente e realizando a pesquisa de referências, quais seriam os principais riscos relacionados às atividades exercidas na organização.

Nessa procura, foi identificado a pesquisa realizada por ALVES, Renato S. & GEORG, Marcus A. C. & NUNES, Rafael R. (2022), que identifica os Riscos de Negócio das atividades principais do Poder Judiciário (Figura 4).

| Número | Risco de Negócio |
|---|---|
| [1] | Divulgação antecipada de votos, determinações ou decisões |
| [2] | Vazamento de informações sigilosas, protegidas por segredo de Justiça ou dados pessoais |
| [3] | Emissão ou alteração não autorizada de determinações ou decisões |
| [4] | Interrupção da prestação jurisdicional |
| [5] | Previsibilidade ou manipulação da distribuição dos processos |
| [6] | Perda de informações |
| [7] | Parcialidade ou favorecimentos pessoais |
| [8] | Assuntos indesejados ou inadequados em determinações e decisões |
| [9] | Julgamentos legítimos, porém, com base em elementos adulterados |
| [10] | Espionagem de outras nações e/ou grupos de interesse |

**Figure 4. Riscos de negócio das atividades principais do Poder Judiciário. Fonte: (ALVES, Renato S. & GEORG, Marcus A. C. & NUNES, Rafael R., p. 10, 2022)**

Além dos riscos de negócio, nessa mesma pesquisa, Clarice conseguiu identificar o vínculo entre os riscos de negócio com os riscos operacionais, derivada da análise das causas e fontes do risco operacional (Figura 5).

| Causas e Fontes do Risco Operacional | Risco Operacional | Risco de Negócio |
|---|---|---|
| Perda de informações durante a elaboração de análises e minutas de decisões<br>Sistema não permitir salvamento automático ou alerta da necessidade salvamento do documento em elaboração<br>Sistema não possibilizar o versionamento de documentos em fase de elaboração, impossibilitando a recuperação de informações modificadas durante a elaboração da minuta | **Cópia de processos e minutas em computadores ou meios de armazenamento pessoais** | [1] [2] |
| Assédio por partes ou interessados em causas<br>Assédio de grupos hacker<br>Assédio de governos estrangeiros<br>Atuação de organizações criminosas<br>Histórico criminoso<br>Insatisfação e desmotivação<br>Problemas emocionais<br>Doenças psicológicas | **Vazamento intencional por pessoas que tenham acesso a documentos ou informações sensíveis** | [1] [2] [10] |
| Desconhecimento dos desenvolvedores em boas práticas de desenvolvimento seguro<br>Falha no processo de revisão e avaliação da qualidade do código<br>Aproveitamento de código de fontes inseguras<br>Não utilização de ferramentas de análise estática de código - SAST<br>Falta de padronização dos sistemas judiciais eletrônicos, dificultando o controle do código-fonte<br>Comprometimento do repositório de código-fonte | **Código-fonte com vulnerabilidades de segurança** | [1] [2] [3] [4] [5] [8] [9] [10] |

**Figure 5. Exemplos de riscos operacionais identificados a partir dos riscos de negócio. Fonte: (ALVES, Renato S. & GEORG, Marcus A. C. & NUNES, Rafael R., p.11, 2022)**

Após esses resultados da pesquisa de ALVES, Renato S. et al. (2022), Clarice já consegue vislumbrar onde os controles de segurança poderiam ser implementados nos processos de negócio priorizados do Tribunal, a fim de fortalecer a segurança destes, prevenindo futuros ataques.

# Departamentos do Tribunal e a Segurança de seus Processos de Negócio

Após a realização das pesquisas, Rodrigo lembrou da necessidade de entender quais seriam as perspectivas de outros departamentos do Tribunal a respeito da implementação dos controles de segurança em seus processos de negócio. Assim, Clarice ficou responsável por realizar entrevistas com esses colaboradores. Nessas entrevistas, ela se deparou com uma diversidade de perspectivas e preocupações em relação à implementação de novos controles de segurança nos processos de negócio.

Alguns colaboradores manifestaram uma compreensível apreensão em relação à possível complexidade e demora que tais mudanças poderiam acarretar nos fluxos de trabalho estabelecidos há anos. Eles temiam que a adoção de novos controles pudesse interferir em suas rotinas diárias e resultar em possíveis resistências operacionais.

Além disso, a estagiária também percebeu uma relutância em relação às potenciais modificações nos sistemas já consolidados no Tribunal. Muitos colaboradores estavam acostumados com as interfaces e funcionalidades existentes, e qualquer alteração poderia gerar desconforto e a necessidade de adaptação a um novo ambiente de trabalho digital.

Apesar da resistência inicial, Clarice percebeu que algumas entrevistas também revelaram uma abertura para compreender a importância da segurança cibernética. Colaboradores mais engajados reconheceram que, embora haja preocupações legítimas em relação à complexidade, a segurança e integridade dos dados do Tribunal são fundamentais para a garantia de um ambiente confiável e protegido contra ameaças digitais.

# Segurança e Eficiência Operacional: uma relação inversamente proporcional

Ao se deparar com a tarefa de pesquisar alternativas de prevenção de futuros ataques cibernéticos no Tribunal Superior, Clarice mergulhou em um dilema intrigante e crucial: a relação inversamente proporcional entre o aumento da segurança cibernética e a perda potencial de eficiência nos processos de negócio.

Clarice compreendia que a implantação de controles de segurança cibernética era fundamental para fortalecer as defesas do Tribunal contra possíveis ataques. A adoção de medidas rigorosas, conforme indicadas por publicações e *frameworks*, como o 'Cyber Security CIS CSC V 8.0' (CIS, 2021), poderia tornar os sistemas mais resistentes e menos vulneráveis a ameaças cibernéticas.

No entanto, Rodrigo levantou a informação de que à medida que os controles de segurança são implementados e a segurança cibernética é reforçada, os processos de negócio tendem a se tornar mais complexos e demorados. A adição de camadas de segurança pode exigir verificações adicionais, etapas de autorização e procedimentos de autenticação, o que pode impactar o fluxo normal das atividades e causar lentidão em alguns processos.

Essa dualidade levou Clarice a uma reflexão profunda sobre como equilibrar a necessidade de segurança cibernética com a eficiência operacional do Tribunal. Afinal, garantir a segurança das informações é essencial para proteger a justiça e a confidencialidade dos processos, mas não se pode ignorar a importância de manter a agilidade e a eficiência nos trâmites judiciais.

Para enfrentar esse desafio, Clarice compreendeu que a abordagem ideal seria encontrar um equilíbrio entre a implementação dos controles de segurança cibernética e a otimização dos processos de negócio. Isso poderia ser alcançado por meio de uma análise

minuciosa e criteriosa da aplicação dos controles, identificando onde a segurança é mais crítica e onde é possível simplificar procedimentos sem comprometer a proteção dos dados. Ou seja, implementar os controles com base no processo de avaliação de riscos. De que adianta a eficiência sem eficácia?

Além disso, ela percebeu a importância de promover uma cultura de conscientização e treinamento para os colaboradores do Tribunal, a fim de garantir que todos estejam alinhados com as medidas de segurança e compreendam sua relevância para a integridade das operações. Não obstante, as lideranças do Tribunal possuem um papel crucial na implementação das medidas de segurança e no equilíbrio com a agilidade das operações.

## Um olhar para fora: Comparando com Outras Organizações

Para completar sua pesquisa, ela decidiu fazer um *benchmark* em algumas empresas brasileiras para analisar como é realizada a prática da segurança da informação. Para isso, analisou-se um artigo feito por Silva Netto, A. D., et al. Silveira, M. A. P. D. (2007) que estuda uma amostra de 43 empresas de pequeno e médio porte no ABC paulista para descobrir quais são os métodos mais comuns e quais são os fatores que motivam ou inibem a adoção da gestão de segurança da informação. Os resultados mostram que as técnicas mais utilizadas são antivírus, backup de arquivos e firewall e os principais fatores desmotivadores são o valor do investimento, a dificuldade de mensurar o custo-benefício, a falta de conhecimento e a própria cultura organizacional das empresas. Por fim, dentre as três camadas da gestão de segurança - física, lógica e humana - a humana é a que se encontra mais deficitária. Há que se fazer o ser humano o elo mais forte da corrente!

Essa pesquisa fez Clarice repensar um pouco sobre a diferença entre

o que ela estudou e o que é executado na prática, uma vez que nem sempre as organizações vão escolher os melhores métodos, seja por não ter recursos ou conhecimento sobre segurança da informação, seja por que vão preferir ter menos segurança, mas em compensação vão ter mais agilidade nos processos.

## Fortalecendo a Segurança Cibernética

Após extensas pesquisas e dedicação, Clarice, a estagiária e Rodrigo, o gerente do Escritório de Gestão de Processos Organizacionais do Tribunal Superior, estavam prontos para consolidar todas as informações em um relatório abrangente. Eles sabiam da importância desse documento para apresentar suas descobertas e propostas a Fernanda, sua supervisora, e Miguel, o chefe do Escritório. O relatório seria uma das referências para direcionar a estratégia de prevenção de futuros ataques cibernéticos e aumentar a segurança dos fluxos de processo de negócio do Tribunal.

Para melhor comunicar suas conclusões, Clarice organizou as informações de forma concisa. Ela enfatizou a importância de uma abordagem equilibrada entre a segurança cibernética e a eficiência nos processos de negócio, mostrando como as lideranças desempenhariam um papel fundamental na tomada de decisões informadas.

Ao chegar à parte crucial do relatório, Clarice apresentou a sugestão de implantação, destacando o 'Modelo de três linhas do IAA 2020' (IAA, 2020). Ela explicou que esse modelo ajudaria o Tribunal a identificar estruturas e processos que auxiliam no atingimento dos objetivos e facilitam uma governança forte e um gerenciamento de riscos eficiente (Figura 6).


**Figure 6. O Modelo das Três Linhas do The IIA. Fonte: (IAA, 2020)**

Clarice descreveu os principais pontos do modelo, incluindo a abordagem baseada em princípios, a ênfase na contribuição do gerenciamento de riscos para a criação de valor e a compreensão clara dos papéis e responsabilidades dentro do modelo.

Além disso, ela destacou a importância de alinhar as atividades e os objetivos com os interesses priorizados dos *stakeholders*, garantindo que o Escritório de Gestão de Processos Organizacionais estivesse comprometido em atender às expectativas daqueles que confiavam na segurança e integridade do Tribunal.

Com o relatório finalizado, Rodrigo, com o apoio da Clarice, estava pronto para apresentá-lo a Fernanda e Miguel. Rodrigo solicitou uma reunião com ambos. Durante a apresentação do relatório, ele destacou a importância crítica da situação, enfatizando que o recente ataque hacker expôs a fragilidade dos sistemas e a necessidade urgente de medidas preventivas mais robustas. Ficou claro que muitos conselhos ainda não estavam preparados para tomar decisões relacionadas à segurança cibernética em níveis mais elevados de administração. Isso levantou preocupações significativas.

Miguel, o chefe do Escritório de Gestão de Processos Organizacionais, concordou com a urgência da situação. Eles perceberam que um trabalho conjunto deveria ser realizado para implementar

as mudanças propostas e fortalecer a segurança cibernética. A possibilidade de novos ataques e suas consequências iminentes tornaram evidente a necessidade de decisões rápidas e eficazes, envolvendo todas as partes interessadas. A equipe estava agora diante de um momento crítico em que medidas decisivas eram essenciais para proteger os sistemas e garantir a continuidade das operações do tribunal.

---

## Perguntas para o debate

1. Quais são os principais desafios enfrentados pelas organizações ao integrar o risco cibernético nas decisões da alta administração e na governança geral?
2. Os resultados da pesquisa de Rodrigo e Clarice foram satisfatórios? Comente o que poderia ter sido realizado para aprimorar a pesquisa realizada.
3. Quais estratégias podem ser adotadas para tornar o Tribunal mais resiliente a futuros ataques cibernéticos, sem comprometer a eficiência dos processos de negócio?
4. Quais as principais lições aprendidas com o ataque hacker anterior e como ela podem ser aplicadas para fortalecer a resiliência do Tribunal contra futuras ameaças cibernéticas?
5. Como pode ser fortalecida a colaboração entre o Escritório de Gestão de Processos Organizacionais e outras áreas do Tribunal, para garantir a implementação efetiva das medidas de segurança cibernética?
6. Considerando a evolução constante das ameaças cibernéticas, como aumentar o preparo do Tribunal para lidar com ataques mais sofisticados no futuro?

7. Como a eficiência de processos de negócio são impactadas pela implementação de medidas de segurança? Nesse cenário, qual é a melhor abordagem: a eficácia ou a eficiência?
8. Como relacionar riscos de negócio a riscos operacionais? Como é possível melhorar a comunicação entre diversos níveis organizacionais no que tange aos riscos?

---

# Nota dos autores

[1]Importante esclarecer que um ataque por meio de um ransomware é empregado em várias fases. Nesse caso de ensino, se optou em simplificar e não se aprofundar nessa questão para fins didáticos.

---

# Galeria

Table 1: Function and Category Unique Identifiers

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

**Figure 7. Funções e categorias do Framework de Cibersegurança NIST. Fonte: NIST CSF (2018)**


**Figure 8. Controles de segurança CIC. Fonte: McClain, S. & Sagerand, T. (2018)**

# STJ diz que sistema de informática do tribunal foi alvo de ataque hacker e pede investigação da PF

Técnicos verificaram indisponibilidade do sistema nesta terça (3). Eles afirmaram ter encontrado arquivo que pode ser vírus. Presidente do STJ decidiu suspender sessões temporariamente.

Por Márcio Falcão e Fernanda Vivas, TV Globo — Brasília

04/11/2020 10h52 · Atualizado há 2 anos

**Figure 9. Notícia. Fonte: Delis Ortiz, TV Globo (2020)**

# PF prende autores de ataques cibernéticos a site mantido pelo STF

Em 23 de março de 2021, três suspeitos exploraram vulnerabilidade no portal da Rádio Justiça, gerenciado pelo Supremo Tribunal Federal

Mirelle Pinheiro, Carlos Carone
07/04/2022 07:24, atualizado 07/04/2022 10:27

**Figure 10. Notícia. Fonte: Mirelle Pinheiro, Carlos Carone, Metrópole (2022)**

---

# Referências

Alves, Renato S.; Georg, Marcus A. C.; Nunes, Rafael R. (2022). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. Monografia - Administração, FACE, Universidade de Brasília - UnB, Brasília. DOI: 10.17013/risti.n.pi-pf. Acesso em: 22, jul. 2023.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 2016. Acesso em 20 de julho de 2023, disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL [lei geral de proteção de dados] (2018). Acesso em 24 de julho de 2023 https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CIS, Center for Internet Security. (2021). "Simplified & Prioritized Cyber Defense Guidance – CIS Critical Security Controls - CSC, Version 8.0". Acesso em 23 de julho de 2023, disponível em: https://www.cisecurity.org/controls

Conselho Nacional de Justiça [CNJ]. (2021a). Estratégia Nacional de Segurança Cibernética do Poder Judiciário. Portaria CNJ n. 162/2021. Acesso em 23 de julho de 2023, disponível em: https://atos.cnj.jus.br/files/compilado1402302021061460c7617672ec5.pdf

Conselho Nacional de Justiça [CNJ]. (2021b). Justiça 4.0. Acesso em 21 de maio de 2022, disponível em https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/

Conselho Nacional de Justiça [CNJ]. (2012). Tribunais Superiores: Quais são? O que fazem?. JusBrasil. Acesso em 22 de julho de 2023, disponível em https://www.jusbrasil.com.br/noticias/tribunais-superiores-quais-sao-o-que-fazem/170117397

FebranTech, (2023). Acesso em 23 de julho de 2023. https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio

Hino, M. C., & Cunha, M. A. (2020). Adoção de tecnologias na perspectiva de profissionais de direito. Revista Direito GV, v. 16(n. 1), e1952. Acesso em 22 de julho de 2023. DOI:10.1590/2317-6172201952.

Lima, Eduardo & Moreira, Fernando & Deus, Flavio & Amvame Nze, Georges & de Sousa Junior, Rafael & Nunes, Rafael. (2022). Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao. E49. 301-312. Acesso em 23 de julho de 2023, disponível em: https://www.researchgate.net/publication/362916438_Avaliacao_da_Rotina_Operacional_do_Operador_Nacional_do_Sistema_Eletrico_Brasileiro_ONS_em_Relacao_as_Acoes_de_Gerenciamento_de_Riscos_Associados_a_Seguranca_Cibernetica

McClain, S. & Sagerand, T. (2018). “Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle”. Acesso em 23 de julho de 2023, disponível em: https:

//www.cisecurity.org/insights/white-papers/auditing-assessing-analyzing-a-prioritized-approach-using-the-pareto-principle

NIST_CSF, Cybersecurity Framework, Version 1.1, (2018). "Framework for Improving Critical Infrastructure Cybersecurity". Acesso em 23 de julho de 2023, disponível em: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

NIST Special Publication (SP) 800-53, Revision 5, (2020). "Security and Privacy Controls for Federal Information Systems and Organizations". Acesso em 23 de julho de 2023, disponível em: https://doi.org/10.6028/NIST.SP.800-53r5

PF prende autores de ataques cibernéticos a site mantido pelo STF, Pinheiro Mirelle,Carone Carlos. Metrópole, 2022. Disponível em: https://www.metropoles.com/distrito-federal/na-mira/pf-prende-autores-de-ataques-ciberneticos-a-site-mantido-pelo-stf. Acesso em 24 de julho de 2023

Polícia Federal identificou hacker que invadiu sistema do STJ, diz diretor-geral Ortiz, Denis. TV Globo, 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/11/06/policia-federal-identificou-hacker-que-invadiu-sistema-do-stj-diz-diretor-geral.ghtml. Acesso em 24 de julho de 2023.

Silva Netto, A. D., & Silveira, M. A. P. D. (2007). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM-Journal of Information Systems and Technology Management, 4, 375-397.

Supremo Tribunal Federal, (2023). Acesso em 23 de julho de 2023 https://portal.stf.jus.br/textos/verTexto.asp?servico=centralDoCidadaoCartaDeServiServicosJurisdicionais&pagina=processosConsultaProcessual

Supremo Tribunal Federal. (2018). Programa Processo Eletrônico: O Supremo em Sintonia com o Futuro. Acesso em 22 de julho de 2023, disponível em https://portal.stf.jus.br/textos/verTexto.asp?servico=processoPeticaoEletronica&pagina=Informacoes_gerais_

apos_desligamento_v1.

The Institute of Internal Auditors [IAA]. (2020). Modelo das Três Linhas do IAA 2020: uma atualização das três linhas de defesa. Acesso em 23 de julho de 2023, disponível em: https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-2020

---

# Sobre os autores

- Gabriel Marinho Godinho é estudante de Administração da Universidade de Brasília, membro da Equipe Casoteca ADM e ex-membro da AD&M Consultoria Empresarial. Possui experiência profissional como Consultor de Projetos, atuando com Gestão Pública e, atualmente, atua como Analista de Processos Organizacionais em uma das maiores corretoras de seguros do Brasil. Email: g.marinho99@gmail.com
- Beatriz Teles Fernandez é estudante de Administração da Universidade de Brasília e membro da Equipe Casoteca ADM. Email: falecombtf@gmail.com
- Renato Solimar Alves é gestor de Segurança da Informação e Tecnologia da informação com atuação na proteção dos recursos tecnológicos no Poder Judiciário há 15 anos. É membro ativo do Comitê Gestor de Segurança da Informação do Poder Judiciário, e contribuiu para a definição e implementação de políticas e diretrizes que fortalecem a postura de segurança cibernética e a resposta a incidentes de segurança no âmbito judiciário. É mestre em Engenharia Elétrica, possui especialização em Engenharia de Sistemas, graduando-se previamente em Tecnologia de Telecomunicações Móveis e contando com formação técnica em eletrônica. Sua experiência inclui a liderança de equipes no setor público e em empresas de telecomunicações.

- Carlos Zottmann é graduado em Tecnologia em Processamento de Dados pelas Faculdades Integradas da Católica de Brasília, e possui MBA em Governança em TI pela Unieuro e Pós-graduação Lato Sensu em Direito Digital e Proteção de Dados pelo IDP. É Certified Information Systems Security Professional (CISSP) pelo ISC2, e atualmente é aluno de Mestrado em Segurança Cibernética na Universidade de Brasília (UnB). Profissional com mais de 30 anos de experiência em TI, tendo atuado primordialmente em órgãos do Poder Judiciário. É servidor do Superior Tribunal de Justiça desde 1994, onde atuou como gestor nas áreas de infraestrutura e segurança cibernética, e encontra-se cedido ao Tribunal Superior Eleitoral desde 2018, onde atua como Chefe do Núcleo Estratégico de Gestão de Segurança Cibernética.
- Rafael Rabelo Nunes é profissional com formação em TI e carreira docente ativa, que busca na sinergia entre tecnologia e pessoas, o motor de transformação das organizações. Atualmente é Professor Adjunto da Universidade de Brasília em regime parcial, onde se dedica à ensinar e pesquisar como a TI pode ser utilizada de maneira estratégica pelas pessoas e pelas organizações, levando em consideração os riscos envolvidos. É Assessor em Gestão de Riscos no Supremo Tribunal Federal, e Professor no Centro Universitário UniAtenas. É Doutor em Engenharia Elétrica pela Universidade de Brasília. Graduado em Engenharia de Redes de Comunicação pela Universidade de Brasília. Email: rafaelrabelo@unb.br
- Editora: Nicole Alonso Santos de Sousa é aluna egressa do Departamento de Administração (ADM/FACE) da Universidade de Brasília (UnB) e Co-coordenadora da Casoteca ADM. Pós-graduação em Finanças e Controladoria (MBA USP/ESALQ). Bacharel em Administração (UnB). Email: nicolealonso2000@gmail.com
- Editor: Luiz Henrique Lima Rodrigues é estudante de Administração da Universidade de Brasília e Co-coordenador da Casoteca ADM. Diretor de Relacionamentos 2024 da Concentro

(Federação das Empresas Juniores do Distrito Federal). Email: luizhenriquelima305@gmail.com.

---

Este caso foi escrito a partir de informações secundárias e com base em outras referências citadas. Não é intenção dos autores avaliar ou julgar a empresa em questão. Este texto é destinado exclusivamente ao estudo e à discussão acadêmica, sendo vedada a sua utilização ou reprodução em qualquer outra forma. A violação aos direitos autorais sujeitará o infrator às penalidades da Lei Nº 9.610/1998.