



## ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO<sup>1</sup>

### 1. Descrição da Solução de Tecnologia da Informação

#### 1.1. Endpoint Protection

Conjunto de módulos de software, que funcionam de forma integrada, com o objetivo de proteger as estações de trabalho (Endpoint Protection) contra eventuais ataques cibernéticos.

#### 1.2. Gateway de e-mail

Solução de segurança de e-mail integrada, incluindo anti-spam, antivírus e outras ferramentas anti-malware.

#### 1.3. Software de backup para Zimbra Open Source Edition

Solução completa de backup e restauração para o Zimbra Open Source Edition.

### 2. Definição e especificação de requisitos

#### 2.1. Endpoint Protection

Os investimentos em segurança cibernética e privacidade exigem das organizações uma maior atenção, diante dos ataques cada vez mais sofisticados. Ameaças e crimes cibernéticos organizados e direcionados preocupam sociedades e organizações. A divulgação de informações críticas de forma indevida e os incidentes de segurança continuam crescendo e atingem todos os tipos de organizações (PWC<sup>2</sup>).

Conforme o United States Computer Emergency Readiness Team (US-CERT<sup>3</sup>) — órgão dos EUA responsável por analisar e reduzir vulnerabilidades e disseminar informações sobre ameaças cibernéticas — uma parte significativa dos códigos maliciosos (vírus, *worms*, *trojans*, *rootkits*, *spywares*, etc) são projetados para contornar os controles de segurança das organizações, furtar e enviar ao atacante informação sensível (US-CERT<sup>2</sup>).

De acordo CERT.BR<sup>4</sup>, códigos maliciosos (*malwares*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- Pela exploração de vulnerabilidades existentes nos programas instalados;

1 Adaptado de “Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação v2.0”; Ministério do Planejamento, Orçamento e Gestão. Disponível em: <<https://www.governoeletronico.gov.br/documentos-e-arquivos/Guia%20de%20Boas%20Praticas%20em%20Contratacao%20de%20Solucoes%20de%20TI.pdf>>.

2 Disponível em: <<https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/cyber-essentials/cyber-essentials-5.pdf>>. Acessado em 19/06/2017.

3 Disponível em: <<https://www.us-cert.gov/sites/default/files/publications/malware-threats-mitigation.pdf>>. Acessado em 19/06/2017.

4 Disponível em: <<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>>. Acessado em 19/06/2017.

- Pela autoexecução de mídias removíveis infectadas, como pendrives;
- Pelo acesso às páginas Web maliciosas, utilizando navegadores vulneráveis;
- Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas;
- Através de mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os *malwares* passam a ter acesso aos dados armazenados no computador e podem executar ações maliciosas em nome dos usuários. (CERT.BR<sup>5</sup>)

Por este motivo, o investimento em capacitação dos colaboradores, a fim de melhorar a compreensão sobre segurança da informação e, ao mesmo tempo, a melhoria dos sistemas de segurança contribuem com a redução de incidentes, e assim, minimizam o vazamento indevido de informação sensível (US-CERT<sup>2</sup>).

Nesse sentido, o NIST<sup>6</sup> propõe estratégias de mitigação de *malwares* em estações de trabalho que, entre outras, contemplam:

1. *Software anti-malware*: Monitora, identifica e remove malwares;
2. *Host-based IPS*: Monitora os eventos de tráfego de rede, arquivos de log, processos em execução, acessos e modificações em arquivos, e alterações na configuração da estação ou dos arquivos de configuração;
3. *Filtro/Inspeção de conteúdo*: Identifica e bloqueia a execução de anexos ou arquivos com código malicioso e extensões de arquivos suspeitas (ex: .txt.vbs, .htm.exe, etc), previne o acesso a conteúdo web inapropriado ao ambiente de trabalho, bem como bloqueia janelas de *popups* indesejadas e ainda pode prover informação de reputação, as quais auxiliam o usuário a identificar endereços web maliciosos antes de acessá-lo;
4. *Whitelist* de aplicação: Especificam quais aplicações estão autorizadas para a estação de trabalho.

### 2.1.1. Necessidades de Negócio

O Tribunal de Contas do Distrito Federal (TCDF) aprecia as contas anuais dos governadores, emitindo parecer para o julgamento na Câmara Legislativa; julga as contas dos administradores e demais responsáveis por dinheiro, bens e valores públicos; confere a legalidade dos atos de admissão de pessoal (concursos públicos e outras contratações) e a concessão de aposentadorias, reformas e pensões dos servidores do GDF; avalia a execução das metas estabelecidas no plano plurianual, nas diretrizes orçamentárias e no orçamento anual (TCDF<sup>7</sup>).

O Plano Diretor de Tecnologia da Informação do TCDF (PDTI-TCDF), biênio 2016-2017, define os seguintes objetivos de TI:

- 5 Disponível em: <<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>>. Acessado em 19/06/2017.
- 6 Disponível em: <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>>. Acessado em 19/06/2017.
- 7 Disponível em: <<http://www.tc.df.gov.br/web/tcdf1/conheca-o-tcdf>>. Acessado em 19/06/2017.

- Acompanhar a evolução tecnológica;
- Garantir a disponibilidade e continuidade dos serviços de TI;
- Promover a segurança da informação.

Considerando o propósito do TCDF, órgão que trabalha essencialmente com informação sensível e/ou sigilosa em seus processos, e o conjunto de ações danosas e atividades maliciosas apresentadas, a aquisição de solução de proteção de estações de trabalho para TCDF, visa contribuir com o atingimento dos objetivos definidos no PDTI-TCDF.

### 2.1.2. Situação do TCDF

Atualmente o TCDF possui aproximadamente 900 estações de trabalho ativas, que estão em uso regular por colaboradores do TCDF. Adicionalmente a estas estações, existe a expectativa de preenchimento por concurso de 108 vagas em cargos efetivos, entre técnicos e analistas, o que amplia a expectativa total de licenças de software antivírus para 1008 licenças.

*Para fins do estudo, considera-se que 1000 licenças atenderão as necessidades do TCDF durante a vigência do futuro contrato.*

### 2.1.3. Requisitos tecnológicos e demais requisitos

Requisito	2.1.3.1
Descrição	Fornecedor deve capacitar a equipe de 8 pessoas, no ambiente do TCDF, para administrar e operar a solução

Requisito	2.1.3.2
Descrição	A resposta à solução de problemas deverá ocorrer no prazo e condições especificados no Termo de Referência.

Requisito	2.1.3.3
Descrição	Fornecedor deve oferecer pelo menos 2 canais de contato para suporte, sendo um deles, obrigatoriamente, o atendimento telefônico.

Requisito	2.1.3.4
Descrição	O fornecedor deve implantar a solução no tempo definido no Termo de Referência, a contar da assinatura do contrato.

Requisito	2.1.3.5
Descrição	O suporte deve ser prestado pelo prazo de vigência do contrato.



## 2.2. Gateway de e-mail

De acordo com o estudo *Fighting Internet spam in Brazil – Historical overview and reflections on combating spam and managing port 25, coordinated by the Brazilian Internet Steering Committee*<sup>8</sup>, publicado pelo Comitê Gestor da Internet do Brasil (CGI.br), “spam é o principal veículo para distribuição de códigos maliciosos e uma séria ameaça à segurança da Internet” (tradução livre).

Ainda de acordo com o estudo, “a luta contra spam vem sendo discutida em fóruns sobre governança e regulação da Internet nos últimos 15 anos” (tradução livre).

Em 2009, o Brasil chegou ao topo do ranking *Composite Blocking List*<sup>9</sup> de nações que mais geram spam. Houve casos de outros países bloquearem a entrada de e-mails provenientes do Brasil apenas pelo critério da nacionalidade.

De acordo com o antispam.br<sup>10</sup>, são problemas causados pelo recebimento de spam:

- I. Não recebimento de e-mails: boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja grande, ele corre o risco de ter sua caixa postal lotada com mensagens não solicitadas; Se isto ocorrer, passará a não receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente;
- II. Gasto desnecessário de tempo: para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal;
- III. Aumento de custos: independente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe;
- IV. Perda de produtividade: para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso;
- V. Conteúdo impróprio ou ofensivo: como a maior parte dos spams é enviada por conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo;
- VI. Prejuízos financeiros causados por fraude: o spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros.

Por fim, outra ameaça que tem assolado as empresas e que também tem sido disseminada por mensagens de correio eletrônico é o *ransomware*.

De acordo com a Cartilha de Segurança para Internet, publicada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

8 Disponível em: <[https://www.cgi.br/media/docs/publicacoes/1/CadernoCGI\\_Estudos1\\_Ingles.pdf](https://www.cgi.br/media/docs/publicacoes/1/CadernoCGI_Estudos1_Ingles.pdf)>. Acessado em 19/06/2017.

9 Disponível em: <[https://en.wikipedia.org/wiki/Composite\\_Blocking\\_List](https://en.wikipedia.org/wiki/Composite_Blocking_List)>. Acessado em 19/06/2017.

10 Disponível em: <<http://antispam.br/problemas/>>. Acessado em: 19/06/2017.

(CERT.br), “*ransomware*<sup>11</sup> é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário”.

Ainda segundo a cartilha, o *ransomware* pode se propagar de diversas formas, embora as mais comuns sejam:

- Através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link;
- Explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Para a proteção contra essa ameaça é necessário tomar os mesmos cuidados para evitar outros códigos maliciosos, quais sejam:

- Manter o sistema operacional e os programas instalados atualizados;
- Ter um antivírus instalado;
- Ser cuidadoso ao clicar em links ou abrir arquivos.

### 2.2.1. Necessidades de Negócio

O Plano Diretor de Tecnologia da Informação do TCDF (PDTI-TCDF), biênio 2016-2017, define os seguintes objetivos de TI:

- Acompanhar a evolução tecnológica;
- Garantir a disponibilidade e continuidade dos serviços de TI;
- Promover a segurança da informação.

Considerando o propósito do TCDF, órgão que trabalha essencialmente com informação sensível e/ou sigilosa em seus processos, e o conjunto de ações danosas e atividades maliciosas apresentadas, a aquisição de solução de segurança para correio eletrônico, visa contribuir com o atingimento dos objetivos definidos no PDTI-TCDF.

### 2.2.2. Situação do TCDF

Atualmente o sistema de correio eletrônico do Tribunal de Contas do Distrito Federal possui a seguinte arquitetura:



**Figura 1** – Esquema do sistema de correio eletrônico do TCDF (entrada de e-mails).

São quatro os componentes básicos do sistema:

- **Mail Transfer Agent (MTA):** É o agente de transferência de e-mails. É um termo genérico para programas, no caso de programas opensource

<sup>11</sup> Disponível em: <<https://cartilha.cert.br/ransomware/>>. Acessado em 19/06/2017.

podemos citar: Sendmail, Postfix ou Qmail, que enviam e recebem e-mails<sup>12</sup>, utilizando a porta SMTP (25) ou SMTPS (465 ou 587). Este programa representa a “borda” do sistema de MTA. Atualmente o Tribunal utiliza o software Postfix<sup>13</sup> para esta função.

- **Antivírus:** Após o recebimento de e-mail, o software responsável por fazer a integração<sup>14</sup> entre o MTA, antivírus e anti-spam encaminha a mensagem para a verificação de códigos maliciosos. O Tribunal utiliza o software ClamAV<sup>15</sup> para detecção de *malwares*<sup>16</sup>.
- **Anti-spam:** Caso a mensagem não contenha características de *malware*, será encaminhada para a verificação de spam, que é realizada pelo software SpamAssassin<sup>17</sup>. Caso a mensagem seja classificada como spam, será bloqueada. Se não for spam, será encaminhada para o servidor de correio eletrônico.
- **Servidor de correio eletrônico:** o servidor de correio eletrônico utilizado pelo Tribunal é o Zimbra Open Source Edition<sup>18</sup>.

Atualmente o TCDF possui 995 caixas de correio eletrônico, entre Conselheiros, servidores efetivos e comissionados, estagiários e caixas das unidades. Adicionalmente a estas caixas, existe a expectativa de preenchimento por concurso de 108 vagas em cargos efetivos, entre técnicos e analistas. Por fim, ultimamente, os estagiários têm recebido mais autorizações das respectivas chefias para terem contas de correio eletrônico e as unidades do Tribunal têm solicitado a criação de contas para finalidades específicas, como, por exemplo, um evento ou uma pesquisa.

*Dessa forma, considera-se que 1.200 licenças atenderão as necessidades do TCDF durante a vigência do futuro contrato.*

### 2.2.3. Requisitos tecnológicos e demais requisitos

Requisito	2.2.3.1
Descrição	Fornecedor deve capacitar a equipe de 8 pessoas, no ambiente do TCDF, para administrar e operar a solução.

Requisito	2.2.3.2
Descrição	A resposta à solução de problemas deverá ocorrer no prazo e condições especificados no Termo de Referência.

12 Disponível em: <[https://www.symantec.com/pt/br/security\\_response/glossary/define.jsp?letter=m&word=mta-mail-transfer-agent](https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=m&word=mta-mail-transfer-agent)>. Acessado em 19/06/2017.

13 Disponível em: <<http://www.postfix.org/>>. Acessado em 19/06/2017.

14 O software que faz a integração se chama AmaViS (A Mail Virus Scanner).

15 Disponível em: <<http://www.clamav.net/>>. Acessado em 19/06/2017.

16 Disponível em: <<https://cartilha.cert.br/malware/>>. Acessado em 19/06/2017.

17 Disponível em: <<http://SpamAssassin.apache.org/>>. Acessado em 19/06/2017.

18 Disponível em: <<https://www.zimbra.com/>>. Acessado em 19/06/2017.





Requisito	2.2.3.3
Descrição	Fornecedor deve oferecer pelo menos 2 canais de contato para suporte, sendo um deles, obrigatoriamente, o atendimento telefônico.

Requisito	2.2.3.4
Descrição	O fornecedor deve implantar a solução no tempo definido no Termo de Referência, a contar da assinatura do contrato.

Requisito	2.2.3.5
Descrição	O suporte deve ser prestado pelo prazo de vigência do contrato.

### 2.3. Software de backup para Zimbra Open Source Edition

Backups (ou cópias de segurança) são extremamente importantes, pois, segundo a Cartilha de Segurança para a Internet, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, permitem:

- Proteção de dados: preservar os dados para que sejam recuperados em situações como falha de disco rígido, atualização malsucedida do sistema operacional, exclusão ou substituição acidental de arquivos, ação de códigos maliciosos/atacantes e furto/perda de dispositivos;
- Recuperação de versões: recuperar uma versão antiga de um arquivo alterado, como uma parte excluída de um texto editado ou a imagem original de uma foto manipulada;
- Arquivamento: copiar ou mover dados que deseja ou que precisa guardar, mas que não são necessários no dia a dia e que raramente são alterados.

#### 2.3.1. Necessidades de Negócio

O Plano Diretor de Tecnologia da Informação do TCDF (PDTI-TCDF), biênio 2016-2017, define os seguintes objetivos de TI:

- Acompanhar a evolução tecnológica;
- Garantir a disponibilidade e continuidade dos serviços de TI;
- Promover a segurança da informação.

Considerando o propósito do TCDF, órgão que trabalha essencialmente com informação sensível e/ou sigilosa em seus processos, e que as informações recebidas via correio eletrônico devem passar por cópia de segurança, a aquisição de solução de backup para o sistema de correio eletrônico do Tribunal, visa contribuir com o atingimento dos objetivos definidos no PDTI-TCDF.

### 2.3.2. Situação do TCDF

O Tribunal possui apenas o *backup full* (completo) das mensagens. Isso significa que, caso o servidor de correio eletrônico fique completamente inoperante, é possível recuperar todas as mensagens do dia anterior. Porém, esse *backup* não é em tempo real e não é granular. Isso significa, respectivamente, que:

- Em caso de falha, as mensagens do dia corrente serão perdidas;
- Caso o usuário delete uma única mensagem da sua caixa postal por engano, não será possível recuperar.

### 2.3.3. Requisitos tecnológicos e demais requisitos

Requisito	2.3.3.1
Descrição	Fornecedor deve capacitar a equipe de 7 pessoas, no ambiente do TCDF, para administrar e operar a solução.

Requisito	2.3.3.2
Descrição	A resposta à solução de problemas deverá ocorrer no prazo e condições especificados no Termo de Referência.

Requisito	2.3.3.3
Descrição	Fornecedor deve oferecer pelo menos 2 canais de contato para suporte, sendo um deles, obrigatoriamente, o atendimento telefônico.

Requisito	2.3.3.4
Descrição	O fornecedor deve implantar a solução no tempo definido no Termo de Referência, a contar da assinatura do contrato.

Requisito	2.2.3.5
Descrição	O suporte deve ser prestado pelo prazo de vigência do contrato.

## 3. Levantamento das soluções disponíveis

Para fins de levantamento de soluções disponíveis no mercado que oferecem proteção de estação de trabalho (*endpoint protection*), utilizou-se como parâmetro a pesquisa efetuada pelo GARTNER<sup>19</sup> que identifica os quatro

<sup>19</sup> Disponível em: <<https://www.gartner.com/doc/3588017/magic-quadrant-endpoint-protection-platforms>>. Acessado em: 19/06/2017.





principais fornecedores. Para *gateway* de correio eletrônico, utilizou-se as soluções das referidas empresas.

### 3.1. Endpoint Protection

Solução	3.1.1
Nome	SMART PROTECTION FOR ENDPOINTS
Fabricante	Trend Micro
Descrição	<p>A solução apresenta as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>• Gerenciamento Central: Gerenciamento centralizado que provê interface única e integrada para gerenciar, monitorar e gerar relatórios das múltiplas camadas de segurança;</li><li>• Segurança de Endpoints: Protege de atacantes utilizando sistemas avançados de defesa contra ameaças, proteção de navegadores web, controles de aplicação, monitoramento de comportamento, proteção contra ameaças web, proteção contra vulnerabilidades, entre outras;</li><li>• Segurança Móvel: Proteção que inclui rastreamento e monitoramento de dispositivos móveis.</li></ul>

Solução	3.1.2
Nome	SOPHOS ENDPOINT PROTECTION
Fabricante	Sophos
Descrição	<p>Funcionalidades:</p> <ul style="list-style-type: none"><li>• Prevenção: Segurança web, reputação de download, bloqueio de url, controle de periféricos, firewall de cliente, prevenção de <i>exploit</i> de navegadores, antimalware, entre outros;</li><li>• Detecção: análise de comportamento de execução, anti-ransomware, detecção de tráfego malicioso;</li><li>• Resposta: Remoção automática de malware, análise de causa raiz, Sophos Clean e o Synchronized Security Heartbeat.</li></ul>

Solução	3.1.3
Nome	KASPERSKY ENDPOINT PROTECTION
Fabricante	Kaspersky
Descrição	<p>Conforme o fornecedor, a proteção é organizada em camadas e apresenta as seguintes funcionalidades:</p> <ul style="list-style-type: none"><li>• Gerenciamento de correções;</li><li>• Gerenciamento de sistemas;</li><li>• Proteção de dados;</li><li>• Segurança Móvel;</li><li>• Controle Web e de Dispositivos;</li><li>• Controle de Aplicações e whitelisting;</li></ul>



	<ul style="list-style-type: none"><li>• Proteção de Servidor de Arquivos;</li><li>• Firewall Pessoal e HIPS;</li><li>• Prevenção Automática de Exploits;</li><li>• System Watcher;</li><li>• Proteção baseada em nuvem;</li><li>• Scanner de heurística;</li><li>• Proteção baseada em assinatura.</li></ul>
--	--

Solução	3.1.4
Nome	SYMANTEC ENDPOINT PROTECTION
Fabricante	Symantec
Descrição	<ul style="list-style-type: none"><li>• Prevenção de intrusão de rede, URL e políticas de firewall: Analisa tráfego de entrada e saída e bloqueia ameaças enquanto elas trafegam pela rede. Regras baseadas em firewall e proteção de navegador protegem contra-ataques web;</li><li>• Controle de comportamento de aplicação: Controla arquivo e acesso a registros e como a execução dos processos é permitida;</li><li>• Controle de Dispositivo: Restringe acesso de dispositivos de hardware e controla que tipos de dispositivos podem transferir ou receber informação;</li><li>• Mitigação de exploit de memória: Neutraliza códigos maliciosos que operam sobre softwares populares que ainda não tenham sido corrigidos pelo fornecedor;</li><li>• Análise de reputação de arquivo: Sistema de reputação desenvolvido pela Symantec que bloqueia proativamente ameaças;</li><li>• Aprendizado de máquina: Diminui a quantidade de falsos positivos;</li><li>• Emulação: Detecta malware durante execução do arquivo em um ambiente simulado, fazendo com que a ameaça entre em ação e revele a sua presença;</li><li>• Proteção Antivírus: Detecção de malware baseada em assinatura e heurísticas avançadas;</li><li>• Monitoramento comportamental: Monitora o comportamento durante a execução de arquivos considerados importantes;</li></ul>

## 3.2. Gateway de e-mail

### 3.2.1. Softwares open source

De acordo com [opensource.com](https://opensource.com), o software *open source* é aquele que qualquer um pode inspecionar, modificar e melhorar<sup>20</sup>.

Além dessas características, segundo o [opensource.org](https://opensource.org)<sup>21</sup>, os termos de distribuição do software *open source* devem seguir alguns critérios, como, por exemplo, redistribuição livre e distribuição do código junto com o software.

20 Disponível em: <<https://opensource.com/resources/what-open-source>>. Acessado em: 19/06/2017.

21 Disponível em: <<https://opensource.org/osd-annotated>>. Acessado em: 19/06/2017.



Solução	3.2.1.1
Nome	MailScanner
Descrição	<p>MailScanner<sup>22</sup> é um sistema de segurança de e-mail <i>open source</i> desenvolvido para <i>gateways</i> de e-mail baseados em Linux. O programa analisa e-mails procurando por vírus, <i>spams</i> e outros <i>malwares</i>.</p> <p>De acordo com o manual<sup>23</sup> da solução, o software controla uma variedade de aplicações <i>open source</i> para analisar e-mails e detectar spam e vírus, quais sejam:</p> <ul style="list-style-type: none"><li>• ClamAV Antivírus;</li><li>• BitDefender Antivírus;</li><li>• SpamAssassin;</li><li>• Pyzor;</li><li>• Razor2;</li><li>• DCC.</li></ul> <p>A última versão do software é a 5.0.3-7, de 14 de agosto de 2016.</p>

Solução	3.2.1.2
Nome	RadicalSpam
Descrição	<p>De acordo com o site da solução<sup>24</sup>, o pacote RadicalSpam é distribuído sob GPL v2, incluindo produtos como Postfix, SpamAssassin, Amavisd-new, ClamAV, Razor, DCC, Postgrey e Bind, provendo SMTP seguro e funcionalidades anti-spam, antivírus, MTA, DNS, Greylisting etc.</p> <p>Uma das inovações do software é forma como é desenvolvido, o que resulta em independência relativa ao sistema hospedeiro. O RadicalSpam permite que o administrador se livre de restrições de instalações que são frequentemente encontradas em soluções <i>open source</i>, especialmente o gerenciamento de dependências.</p> <p>RadicalSpam pode ser executado nas distribuições Linux mais comuns, como, por exemplo, Redhat, Suse, Gentoo, Debian.</p> <p>A sustentabilidade do sistema é assegurada pela comunidade de usuários, mas também pelas respectivas comunidades de</p>

22 Disponível em: <<https://www.mailscanner.info/>>. Acessado em: 19/06/2017.

23 Disponível em: <<https://s3.amazonaws.com/mailscanner/docs/ms-admin-guide.pdf>>. Acessado em: 19/06/2017.

24 Disponível em: <<https://www.radical-spam.org/en/presentation/>>. Acessado em: 19/06/2017.



	cada produto incluído no pacote.
--	----------------------------------

Solução	3.2.1.3
Nome	SpamAssassin e ClamAV
Descrição	<p>Conforme foi verificado, mesmo aplicações um pouco mais elaboradas (como as apresentadas anteriormente), para fazer verificações de vírus e spam, utilizam, respectivamente, o antivírus ClamAV e o anti-spam SpamAssassin. Na prática, grande parte dos desenvolvedores de softwares <i>open source</i> apenas inserem esses dois programas em suas aplicações e fazem alterações nas interfaces gráficas.</p> <p>O ClamAV é o padrão <i>open source</i> para análises e verificações de e-mails. O software inclui um <i>scanner multi-threaded</i>, utilidades de linha de comando para escaneamento de arquivos <i>on demand</i> e atualizações automáticas de assinaturas de vírus. O programa ainda suporta múltiplos formatos de arquivos, descompactação de arquivos e diferentes linguagens de assinatura. A última versão do software é a 0.99.2, de 03/05/2016.</p> <p>O software SpamAssassin é a plataforma anti-spam open source número um do mercado, dando a administradores de sistemas um filtro para classificar e bloquear e-mails não solicitados. O programa utiliza um <i>framework</i> robusto para atribuir notas aos e-mails e <i>plugins</i> para integrar uma grande quantidade de análises heurísticas e estatísticas nos cabeçalhos e corpos dos e-mails, incluindo análise de texto, filtro de Bayes, listas de bloqueio de DNS e bases de dados colaborativas. SpamAssassin é um projeto da <i>Apache Software Foundation</i> (ASF).</p>

### 3.2.2. Softwares proprietários

Softwares proprietários são programas licenciados, com direitos exclusivos para o produtor. O software, normalmente, é abrangido por patentes e direitos autorais.

Os programas de antivírus e de anti-spams, em sua maioria, são softwares desenvolvidos por empresas especializadas em segurança e que fornecem suporte técnico.

Solução	3.2.2.1
Nome	SYMANTEC MESSAGING GATEWAY
Fabricante	Symantec
Descrição	O Symantec Messaging Gateway permite que as empresas



	<p>protejam seu e-mail e infraestrutura com proteção anti-malware eficaz, precisa e em tempo real, proteção contra ataques direcionados, filtragem de conteúdo avançada, prevenção contra perda de dados e criptografia de e-mail<sup>25</sup>.</p> <p>O software utiliza o Disarm, uma tecnologia proprietária da Symantec, para ajudar a proteger contra ataques direcionados e malware de dia zero, removendo conteúdos exploráveis de anexos do Microsoft Office e PDFs. O documento limpo é reconstruído, reanexado ao e-mail e enviado ao seu destino.</p> <p>O programa também oferece tecnologias avançada para filtragem de conteúdo e para prevenção de perda de dados.</p> <p>O Messaging Gateway oferece um console unificado para gerenciar vários <i>appliances</i>, rastrear mensagens, além de exibir tendências, estatísticas de ataques e incidentes de não conformidade. A aplicação está disponível como um <i>appliance</i> físico ou virtual, usando os ambientes virtuais do VMWare ou Microsoft Hyper-V. É compatível com redes IPv4, IPv6 e mistas e a autenticação LDAP permite login único e configuração de políticas usando grupos LDAP.</p> <p>A Symantec Global Intelligence Network confere mais de 3 bilhões de mensagens por dia para identificar malware e spam com precisão.</p> <p>A Reputação de URLs bloqueia mensagens com links maliciosos.</p>
--	--

Solução	3.2.2.2
Nome	SECURE E-MAIL GATEWAY
Fabricante	Sophos
Descrição	<p>Com a utilização desse programa, segundo a empresa desenvolvedora<sup>26</sup>, é possível proteger os usuários contra o roubo de identidade, senhas, golpes bancários e outros incidentes. É possível interceptar todos os e-mails contendo conteúdo suspeito, anexos ou URLs.</p> <p>O software utiliza a mais recente tecnologia de detecção antivírus e <i>phishing</i>, que é atualizada constantemente em tempo real para detectar as ameaças mais recentes.</p> <p>Sophos Sandstorm estende a segurança convencional, melhorando a proteção, visibilidade e análise de <i>ransomware</i> e ataques direcionados.</p>

25 Disponível em: <<https://www.symantec.com/pt/br/products/messaging-security/messaging-gateway>>. Acessado em: 19/06/2017.

26 Disponível em: <<https://www.sophos.com/en-us/products/secure-email-gateway.aspx#globalsitesfooter>>. Acessado em: 19/06/2017.



	<p>A proteção Time-of-Click da Sophos bloqueia as URLs de e-mails mal-intencionados, para proteger contra ataques de phishing. Toda vez que um link de e-mail é clicado, em qualquer dispositivo, sua reputação é verificada no banco de dados Sophos SXL.</p> <p>Com relação aos <i>spams</i>, a filtragem de reputação bloqueia 90% dos <i>spams</i> no <i>gateway</i> de e-mail, antes que consuma qualquer recurso de rede. Os filtros de chegada de e-mail utilizam uma variedade de métodos avançados de detecção, através de várias linguagens.</p> <p>Também é possível criptografar e assinar digitalmente e-mails sensíveis, de forma automática e transparente. Com DLP também é possível evitar o vazamento inadvertido de dados. Os corpos e anexos das mensagens são automaticamente escaneados para procurar informações sensíveis e é possível estabelecer políticas que determinem se esses e-mails são bloqueados ou encriptados.</p>
--	---

Solução	3.2.2.3
Nome	SECURE MAIL GATEWAY
Fabricante	Kaspersky
Descrição	<p>O Kaspersky Secure Mail Gateway oferece um sistema de e-mail e uma solução de segurança de e-mail totalmente integrados, incluindo anti-spam, antivírus e outras ferramentas antimalware<sup>27</sup>.</p> <p>O software combina métodos de detecção de spam tradicionais com a tecnologia da Kaspersky Lab, que ajuda a bloquear mais spams sem gerar um nível elevado de falsos positivos. As tecnologias incluem:</p> <ul style="list-style-type: none"><li>• Análise de assinatura de texto;</li><li>• Linguística heurística;</li><li>• Métodos com base em DNS;</li><li>• Análise de atributos formais de mensagens;</li><li>• Criação de blacklists e whitelists;</li><li>• Tecnologia de assinatura gráfica;</li><li>• Filtragem de reputação;</li><li>• Sistema de Detecção Urgente 2;</li></ul>

<sup>27</sup> Disponível em: <<https://www.kaspersky.com.br/small-to-medium-business-security/mail-security-appliance>>. Acessado em: 19/06/2017.



	<ul style="list-style-type: none"><li>• Serviço de Atualização Anti-spam Obrigatória (EASUS).</li></ul> <p>Com o uso de dados de reputação fornecidos pela Kaspersky Security Network com base na nuvem, o software classifica automaticamente os e-mails recebidos. E-mails suspeitos são enviados para a quarentena e verificados novamente quando houver informações de reputação atualizadas disponíveis.</p> <p>O filtro de URL recebe atualizações em tempo real sobre a reputação dos URLs fornecidas pela Kaspersky Security Network, com base na nuvem, e ajuda a bloquear e-mails que contêm links para sites infectados.</p> <p>O Sistema de Detecção Urgente (UDS), utiliza um novo tipo de assinatura, chamado Shingle, para ajudar a aumentar a proteção contra novos spams. O UDS 2 bloqueia novos spams sem requerer 100% de correspondência entre as mensagens de spam e o shingle relevante. Mesmo versões modificadas da mensagem de spam serão bloqueadas.</p> <p>O Serviço de Atualização Anti-spam Obrigatória (EASUS) oferece atualizações diretamente da nuvem. Em geral, o EASUS reduz a janela de atualização de spams de 20 minutos para menos de 1 minuto.</p> <p>O Analisador Heurístico utiliza a metodologia de área restrita para permitir a análise de códigos possivelmente maliciosos, para ajudar a detectar novas ameaças antes que uma nova assinatura de malware seja adicionada ao banco de dados antimalware.</p> <p>O filtro de reputação de arquivos também recebe atualizações em tempo real sobre a reputação de arquivos fornecida pela Kaspersky Security Network, para bloquear e-mails que contenham arquivos maliciosos.</p>
--	--

Solução	3.2.2.4
Nome	INTERSCAN MESSAGING SECURITY
Fabricante	Trend Micro
Descrição	<p>Segundo o site da solução<sup>28</sup>, o InterScan Messaging Security fornece segurança totalmente integrada e multicamadas que começa filtrando spams e e-mails maliciosos na nuvem. No nível seguinte, ele consulta as bases de dados de reputação na nuvem e realiza uma varredura final no perímetro da rede.</p> <p>O pré-filtro SaaS opcional para implementações de <i>appliance</i> virtual e software corta os volumes totais de e-mails em até</p>

28 Disponível em: <<http://www.trendmicro.com.br/br/grandes-empresas/seguranca-de-mensagens-rede-web/intercan-message-security/index.html#como-ele-funciona>>. Acessado em: 19/06/2017.





	<p>95%, bloqueando ameaças e spams na nuvem – mais perto de suas origens.</p> <p>Com a tecnologia Smart Protection Network, a Reputação Web e a Reputação de e-mail bloqueiam novas ameaças antes que arquivos de assinaturas estejam disponíveis.</p> <p>A Reputação de Web e E-mail garantem uma proteção imediata ao consultar em tempo real a Trend Micro Smart Protection Network. Baseado em uma inteligência de ameaças na nuvem atualizada a cada minuto, a Reputação de e-mail bloqueia e-mails enviados por fontes conhecidas de spams e cibercriminosos, e a Reputação Web bloqueia o acesso a sites maliciosos.</p> <p>O InterScan Messaging Security pode ser implementado como um <i>appliance</i> de software ou virtual, ou ainda como uma solução de software para Windows e Linux.</p>
--	--

### 3.3. Software de backup para Zimbra Open Source Edition

Solução	3.3.1
Nome	ZIMBRA BACKUP PLUS
Fabricante	Zimbra
Descrição	<p>Zimbra Suite Plus<sup>29</sup> é o complemento modular que permite expandir os recursos do Zimbra Open Source ou Network Edition.</p> <p>Os módulos que podem ser adicionados são:</p> <ul style="list-style-type: none"><li>• Zimbra Backup Plus;</li><li>• Zimbra Admin Plus;</li><li>• Zimbra HSM Plus;</li><li>• Zimbra Mobile Plus.</li></ul> <p>De acordo com o site da solução<sup>30</sup>, o Zimbra Backup Plus é uma solução completa de restauração e backup para o Zimbra.</p> <p>O módulo possui várias opções de restauração, podendo recuperar um único item ou performar uma recuperação de desastre completa.</p> <p>Todas os modos de recuperação são transparentes ao usuário final e são, segundo o site da solução, 100% independentes do sistema operacional e da arquitetura.</p> <p>O Zimbra Backup Plus permite fazer uma imagem completa do sistema de correio eletrônico e armazenar em qualquer lugar.</p>

<sup>29</sup> Disponível em: <<https://www.zimbra.com/zimbra-suite-plus/>>. Acessado em: 19/06/2017.

<sup>30</sup> Disponível em: <<https://www.zimbra.com/zimbra-suite-plus/zimbra-backup-plus/>>. Acessado em: 19/06/2017.



	Os backups são feitos em tempo real, ou seja, assim que os e-mails chegam, já passam por cópia de segurança.
--	--

Solução	3.3.2
Nome	ZTOOL
Fabricante	F13
Descrição	<p>O Ztool é um pacote de ferramentas que acrescenta novas funcionalidades ao Zimbra Open Source Edition.</p> <p>Com esse software é possível adicionar ao Zimbra:</p> <ul style="list-style-type: none"><li>• Backup Online;</li><li>• Auditoria e Archiving;</li><li>• Sincronização com Active Directory;</li><li>• Mobilidade.</li></ul> <p>Utilizando o módulo de backup online, as cópias de segurança são realizadas em tempo real, sem impacto para o Zimbra<sup>31</sup>.</p> <p>Os backups são feitos em tempo real, ou seja, assim que os e-mails chegam, já passam por cópia de segurança.</p> <p>O Ztool realiza deduplicação de mensagens, otimizando o armazenamento.</p>

#### 4. Detalhamento das alternativas existentes

##### 4.1 Detalhamento das alternativas existentes de Endpoint Protection

**Tabela 4.1.1** – Detalhamento da solução SMART PROTECTION FOR ENDPOINTS

SMART PROTECTION FOR ENDPOINTS – Trend Micro			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

31 Disponível em: <[https://www.ztool.com.br/backup\\_online/](https://www.ztool.com.br/backup_online/)>. Acessado em: 19/06/2017.

**Tabela 4.1.2** – Detalhamento da solução SOPHOS ENDPOINT PROTECTION

SOPHOS ENDPOINT PROTECTION - Sophos			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.1.3** – Detalhamento da solução KASPERSKY ENDPOINT PROTECTION

KASPERSKY ENDPOINT PROTECTION - Kaspersky			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.1.4** – Detalhamento da solução SYMANTEC ENDPOINT PROTECTION

SYMANTEC ENDPOINT PROTECTION - Symantec			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

## 4.2 Detalhamento das alternativas existentes de Gateway de correio eletrônico

**Tabela 4.2.1 – Detalhamento da solução MAILSCANNER**

MAILSCANNER			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	-	X <sup>32</sup>	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	X	-	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.2.2 – Detalhamento da solução RADICALSPAM**

RADICALSPAM			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	-	X <sup>33</sup>	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	X	-	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.2.3 – Detalhamento das soluções SPAMASSASSIN e CLAMAV**

SPAMASSASSIN e CLAMAV			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	X	-	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

32 Nas pesquisas realizadas não foram encontradas referências deste software em órgãos da Administração Pública.

33 Nas pesquisas realizadas não foram encontradas referências deste software em órgãos da Administração Pública.

**Tabela 4.2.4 – Detalhamento da solução SYMANTEC MENSSAGING GATEWAY**

SYMANTEC MENSSAGING GATEWAY - Symantec			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.2.5 – Detalhamento da solução INTERSCAN MESSAGING SECURITY**

INTERSCAN MESSAGING SECURITY – Trend Micro			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.2.6 – Detalhamento da solução SECURE E-MAIL GATEWAY**

SECURE E-MAIL GATEWAY – Sophos			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.2.7 – Detalhamento da solução SECURE MAIL GATEWAY**

SECURE MAIL GATEWAY – Kaspersky			
---------------------------------	--	--	--



Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

### 4.3 Detalhamento das alternativas existentes de Backup

**Tabela 4.3.1 – Detalhamento da ZTOOL**

ZTOOL - F13			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

**Tabela 4.3.2 – Detalhamento da ZIMBRA BACKUP PLUS**

ZIMBRA BACKUP PLUS - Zimbra			
Requisito	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X	-	-
A solução está disponível no Portal de Software Público Brasileiro?	-	X	-
A Solução é um software livre ou software público?	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X	-	-
A Solução é aderente às regulamentações da ICP-Brasil?	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	-	-	X

### 5. Justificativa da solução escolhida

Entre as opções de soluções *open source* e proprietárias, optou-se pelo software proprietário pelos seguintes motivos:

- Os softwares proprietários analisados possuem uma série de funcionalidades que atenderão as necessidades de segurança da informação do Tribunal;
- As soluções de segurança para *endpoint* e correio eletrônico, quando do mesmo fabricante, possuem console de administração integrada;
- As soluções estudadas reduzem o tempo de resposta a incidentes de segurança da informação;
- As soluções possuem suporte especializado em segurança da informação.

Por sua vez, com relação à divisão da solução de tecnologia da informação, optou-se pela divisão da seguinte forma:

- item 1: solução de segurança para estações de trabalho (endpoint protection) e para correio eletrônico (gateway);
- item 2: solução de backup para Zimbra Open Source Edition.

A contratação das soluções de segurança da informação para endpoint e correio eletrônico em um único item e do mesmo fabricante justifica-se pela necessidade de integração entre os módulos, possibilitando uma visão unificada, rápida e precisa quanto ao estado de segurança da informação do Tribunal, sem a necessidade de nenhum custo adicional referente à normatização das informações, pois todos os produtos trabalham dentro de um mesmo padrão de informação.

A divisão dessa solução poderia trazer dificuldades na leitura de um cenário de segurança, no qual cada software (de empresas e fabricantes diferentes), que não funciona de forma integrada, poderia ter metodologias, termos e interpretações distintas quanto ao mesmo incidente de segurança, o que acarretaria lentidão na resposta a incidentes.

Por fim, faz-se necessário a análise dos valores, percebendo a vantajosidade de se comprar as soluções de segurança da informação para *endpoint* e correio eletrônico em um único item:

Proposta DFTI Tecnologia da Informação<sup>34</sup>:

- Apenas para proteção de *endpoint*: R\$ 378.900,00
- Apenas para proteção de correio eletrônico: R\$ 229.280,00

<sup>34</sup> e-DOC: D040E136, B4DBED03.





- Para *endpoint* e correio eletrônico em um único item: R\$ 549.000,00

Proposta SdREDES Segurança de Redes<sup>35</sup>:

- Apenas para proteção de *endpoint*: R\$ 268.570,00
- Apenas para proteção de correio eletrônico: R\$ 411.840,00
- Para *endpoint* e correio eletrônico em um único item: R\$ 586.040,00

Proposta InfoDrive Tecnologia<sup>36</sup>:

- Apenas para proteção de *endpoint*: R\$ 103.880,00
- Apenas para proteção de correio eletrônico: R\$ 61.956,00
- Treinamento: R\$ 9.026,40
- Para *endpoint* e correio eletrônico em um único item: R\$ 267.170,40

**Média dos valores para endpoint e correio eletrônico em um único item: R\$ 467.403,46**

Ressalta-se que os representantes da Symantec pesquisados pelo Tribunal não mostraram interesse em encaminhar as cotações solicitadas. As primeiras tentativas de obtenção de cotações datam do mês de março e, até o momento (julho), nenhum representante da Symantec encaminhou os valores para o Tribunal, conforme pode ser verificado por meio dos e-DOCs E6F69E0B, 3FD0DD06, 88CD1C02, 8D9D5B1C, 3A809A18, E3A6D915, 54BB1811, E9065729, 5E1B962D.

Por fim, como o Tribunal, possui dois links de acesso à Internet e, conseqüentemente, dois caminhos para recebimento e envio de e-mails, será solicitado que sejam instalados dois gateways de correio eletrônico, sendo um para cada link. As empresas pesquisadas informaram que essa solicitação não dobrará a cotação para a solução de segurança de correio eletrônico, conforme pode ser verificado por meio dos e-DOCs 73186D0C, CB9B5EA8, 175A477A, 1DFAC946.

Com relação à solução de backup para o Zimbra Open Source Edition, analisou-se duas soluções com funcionalidades equivalentes, porém, após o recebimento das estimativas de preços, percebeu-se que a ferramenta Ztool é mais vantajosa para o Tribunal.

ZTOOL:

- Proposta F13 Tecnologia : R\$ 50.641,00<sup>37</sup>

<sup>35</sup> e-DOC: 73AF70CD, 12643BE6, 17ED5ABB.

<sup>36</sup> e-DOC: CB2C4369.

<sup>37</sup> E-DOC: 35C74EFB.



- Proposta System Way Informática: R\$ 52.740,00<sup>38</sup>
- Proposta Byte Secure: R\$ 54.600,00<sup>39</sup>
- **Média dos valores da solução: R\$ 52.660,33**

Zimbra Backup Plus:

De acordo com site da solução Zimbra, no Brasil, existem 4 (quatro) revendedores<sup>40</sup> da solução em análise. Porém, também foram encontrados problemas para obter as cotações. Conforme pode ser verificado pelos e-DOCs 569C6755, E181A651 e 38A7E55C, apenas uma empresa (que está localizada em Brasília) encaminhou cotação. Além dos e-mails encaminhados, foram feitas ligações telefônicas para as empresas, porém sem resultados.

- Proposta BKTECH: R\$ 306.000,00<sup>41</sup>
- **Média dos valores da solução: 306.000,00**

## 5.1 Solução escolhida

Considerando as soluções analisadas neste processo, as justificativas apresentadas no item anterior e os valores apresentados, para o item 1 (solução de segurança para estações de trabalho (endpoint protection) e para correio eletrônico (gateway)) optou-se por manter a licitação aberta para qualquer solução que atenda a especificação do Termo de Referência. Porém, as soluções deverão ser do mesmo fabricante e ter interface de gerência única. Para o item 2, optou-se pela solução ZTOOL.

## 5.2 Benefícios esperados

- Disponibilizar aos colaboradores estações de trabalho com nível de segurança adequado;
- Controlar e monitorar os softwares instalados ou periféricos que acessam as estações de trabalho;
- Controlar, monitorar e filtrar as páginas web visitadas;
- Aumentar a proteção da rede interna do TCDF contra incidentes de segurança originados nas estações de trabalho.
- Aumentar a proteção contra ataques originados no correio eletrônico;
- Fornecer backup granular para as mensagens de correio eletrônico.

## 6. Necessidades de adequação do ambiente

<sup>38</sup> e-DOC: E64183CA.

<sup>39</sup> e-DOC: 515C42CE.

<sup>40</sup> Disponível em: <<https://www.zimbra.com/partners/resellers/>>. Acessado em: 03/07/2017.

<sup>41</sup> e-DOC: 51EB5F0F.



Necessidade	Adequação de infraestrutura de TI.
Descrição	Para a instalação da solução de proteção de endpoint, será necessário desinstalar a solução anterior.

Necessidade	Adequação de infraestrutura de TI.
Descrição	Para a instalação do módulo de backup do Zimbra, é recomendável a atualização da versão utilizada pelo Tribunal.

Necessidade	Adequação de infraestrutura de TI.
Descrição	Disponibilização de ambiente virtualizado para os fornecedores.

## 7. Recursos necessários à continuidade do negócio

### 7.1 Recursos materiais

Recurso	Máquinas virtuais
Quantidade	Quatro
Disponibilidade	Devem estar disponíveis na data acordada com os fornecedores das soluções
Responsável	Serviço de Infraestrutura de TI

### 7.2 Recursos humanos

Função	Administrador do endpoint protection
Formação	Tecnologia da Informação
Atribuições	Administrar a solução
Carga Horária	5hs semanais

Função	Administrador do gateway de correio eletrônico
Formação	Tecnologia da Informação
Atribuições	Administrar a solução
Carga Horária	5hs semanais

Função	Administrador do backup do Zimbra
--------	-----------------------------------



Formação	Tecnologia da Informação
Atribuições	Administrar a solução
Carga Horária	5hs semanais

Função	Suporte das empresas contratadas
Formação	Tecnologia da Informação
Atribuições	Fornecer suporte aos servidores do Tribunal que administram a solução
Carga Horária	Sob demanda

Função	Serviço de Suporte ao Usuário Final
Formação	Tecnologia da Informação
Atribuições	Fornecer suporte aos servidores do Tribunal, identificando possíveis problemas e comunicando aos administradores das soluções.
Carga Horária	Sob demanda

## 8. Declaração de viabilidade da contratação

De acordo com o inciso VIII do Artigo 12º da IN 4/2014, os integrantes requisitante e técnico da Equipe de Planejamento declaram a viabilidade da contratação aqui analisada.

## 9. Declaração de conformidade

De acordo com o art. 12 da Instrução Normativa MP/SLTI nº 04/2014, assinam este documento os Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação.

**Brasília, 10 de julho de 2017.**

Área	Nome	Matrícula
Requisitante	Alessandro Salomão Gonçalves	1674-2
Técnica	Leonardo Ramos Paz	1510-0
	Miguel Kojio Nobre	1539-6