ITEM	Descrição	OBS		RESPOSTAS GTI- PGE.
1.1 (tabela)	Licença de Software para Servidor de Administração e Console central da solução.	Alterar	Licença de Administração e Console central da solução.	Não será atendida a solicitação de mudança de especificação técnica. Pois, o atual está de acordo com a necessidade e ao que está sendo proposto na especificação técnica.
6.1.3	Firewall de host	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para o endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.1.4.3.2	Mac OS X 10,12,13,14+	Alterar	Mac OS X 10.3,12,13,14+	Esta solicitação será atendida, ou seja, promoveremos a alteração nesse item da Especificação Técnica a fim detalhar e não gerar dúvida técnica.
6.1.5	A solução deve permite testar arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;	Alterar	Permitir enviar arquivos suspeitos para o laboratório de inteligência do fabricante	Não será atendida a solicitação de mudança de especificação técnica. Pois, reduz o escopo de proteção do endpoint. É necessário que a solução seja abrangente com todas as opções solicitadas.
6.2.2.1	Console Central de Gerenciamento	Alterar	Console Central de Gerenciamento on premisses ou em nuvem do fabricante	Esta solicitação será atendida parcialmente, ou seja, promoveremos a alteração nesse item da Especificação Técnica a fim de não gerar dúvida técnica. A solução que se pretende é on premise. Ou seja, está descartada a solução em nuvem.
6.2.2.8	Criar painéis de controle;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para o endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.9.	Capacidade de gerenciar (Windows, Linux e Mac) e servidores (Windows e Linux) protegidos pela solução antivírus;	Alterar	Capacidade de gerenciar (Windows e Mac) e servidores (Windows e Linux) protegidos pela solução antivírus	Esta solicitação será atendida, ou seja, promoveremos a alteração nesse item da Especificação Técnica.

6.2.2.14	Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.15	Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção automaticamente;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.16	Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção automaticamente	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.17	Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o agente e o antivírus automaticamente	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.19	Capacidade de definir políticas de configurações diferentes por grupos de dispositivos de computação, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;	Alterar	Capacidade de definir políticas de configurações diferentes por grupos de dispositivos de computação	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para a administração do endpont.

6.2.2.30	Data e horário de quando a máquina foi ligada;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.38	Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.39	Informação completa de hardware contendo: processadores, memórias, adaptadores, etc.;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica a fim de aumentar a competitividade do Certame.
6.2.2.49	Capacidade de herança de tarefas e políticas na estrutura hierárquica dos dispositivos gerenciados;	Alterar	Capacidade de criação de regras por usuários, dispositivos e grupos.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da solução de proteção do endpoint.
6.2.2.50	Multicast, tecnologia para distribuição local de software, economizando tráfego em escritórios remotos	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.51	Capacidade de eleger automaticamente qualquer dispositivo de computação cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;	Alterar	Capacidade de ter um ponto central como repositório de vacinas e de pacotes de instalação onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para a otimização do tráfego da rede.

6.2.2.54	Capacidade de gerar traps SNMP	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpont e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.2.2.55	Capacidade de ligar, desligar, reiniciar máquinas e também via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;	Retirar	Capacide de desligar e reiniciar máquinas para realização de tarefas (varredura, atualização, instalação, etc), inclusive máquinas que estejam em subnets diferentes do servidor;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da solução.
6.2.2.56	Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);	Alterar	Em caso de epidemia o Endpoint deve ser capaz de se auto isolar de forma a não se proliferar pela rede.	Não será atendida a solicitação de mudança de especificação técnica. Pois é um requisito importante para administração da solução.
6.2.2.59	Capacidade de diferenciar máquinas virtuais de máquinas físicas	Alterar	Capacidade de diferenciar estação de trabalho e servidor.	Este item irá permanecer na forma especificada. É necessário que solução seja abrangente com todas as opções solicitadas.
6.2.2.60	Deve permitir pesquisas baseados nos seguintes critérios: Nome parcial ou completo dos dispositivos de computação, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina, nome do usuário (login usuário do AD), IP e range de IPS (subnet);	Alterar	Deve permitir pesquisas baseados nos seguintes critérios: Nome parcial ou completo dos dispositivos de computação, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina, nome do usuário(login usuário do AD) e IP;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da solução.
6.2.2.61	Deve ter a possibilidade de exportar/importar configurações dos softwares através da console de gerenciamento;	Retirar	A solução (em nuvem) não necessita de backup	Não será atendida a solicitação de mudança de especificação técnica. Pois, não há previsão que possibilite serviços em nuvem.
6.3	PROTEÇÃO ANTIMALWARE OTIMIZADA PARA VIRTUALIZAÇÃO	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.

6.3.2	Requer softwares corporativos de Antivírus especialmente otimizada para funcionar em conjunto com soluções de virtualização, por agentless ou contendo um agente otimizado e com requisitos reduzidos de recursos;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.3.7	Deverá ter controle sobre as maquinas que estão em um mesmo hypervisor de modo que as mesmas não executem o scan de maneira simultânea para não afetar a performance do sistema;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois é um requisito importante para proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE para atender as necessidades, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.3.10	Deverá descobrir e importar maquinas virtuais, tanto as que estejam rodando quanto as que se encontram paradas;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.3.16	Deverá fazer a gestão e alocação de maquinas virtuais automaticamente para os scan com base na carga, pré-configuração ou a ranges de IP;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.3.21	A solução deverá definir uma política por máquina virtual;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.

6.4.3	Antivírus de E-mail (verificação de e-mails recebidos e enviados, assim como seus anexos); compatibilidade com Exchange Active Sync;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.6	Multicast, tecnologia para distribuição local de software, economizando tráfego em escritórios remotos;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.15	Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.16	Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;	Alterar	Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint.
6.4.17	Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “SMTP”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;	Alterar	Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint.
6.4.19	Capacidade de parar automaticamente varreduras agendadas;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.

6.4.23	Capacidade de agendar uma pausa na verificação;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.
6.4.25	Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.26	O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	a) Perguntar o que fazer, ou;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.27	Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);	Alterar	Apagar o objeto ou tentar desinfectá-lo	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint .
6.4.28	Caso positivo de desinfecção:			
	Restaurar o objeto para uso.	Alterar	Restaurar o objeto para uso automaticamente.	Esta solicitação será atendida, ou seja, promoveremos a alteração no item da Especificação Técnica a fim detalhar e não gerar dúvida técnica.
6.4.31	Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.

6.4.32	Capacidade de verificar tráfego de mensagem instantânea contra vírus e links phishings;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.33	Capacidade de verificar links inseridos em e-mails contra phishings;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.36	No e-mail, ao encontrar um objeto potencialmente perigoso, deve:	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
	a) Perguntar o que fazer, ou;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
	b) Bloquear o e-mail.	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.39	a) Restaurar o e-mail para o usuário.	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveemos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.41	Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.42	Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;	Alterar	Capacidade de filtrar anexos de e-mail	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.45	Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica, visto que há outra solução recentemente implantada na PGE que poderá realizar essa funcionalidade.
6.4.46	Na verificação de tráfego web, caso encontrado código malicioso o programa deve:			

	a) Perguntar o que fazer, ou;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	c)Permitir acesso ao objeto.	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.51	Deve ser possível alterar o período que o cache será armazenado para que seja criada uma nova base de assinaturas;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.53	Deve ser possível que analise qualquer tentativa de edição, exclusão ou gravação do registro, automaticamente e que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;	Alterar	Deve ser possível que analise qualquer tentativa de edição, exclusão ou gravação do registro, automaticamente	Esta solicitação será atendida, ou seja, promoveremos a alteração nesse item da Especificação Técnica a fim detalhar e não gerar dúvida técnica.
6.4.54	Deve ser possível bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group;	Alterar	Deve ser possível bloqueio de Phishing	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint.
6.4.55	Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, a Mcafee e a Kaspersky possuem o referido recurso tecnológico.

6.4.56	Deve possuir IDS/IPS, proteção contra port scans. A base de dados de análise deve ser atualizada juntamente com as vacinas	Alterar	Deve possuir IDS/IPS	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração e atualização de proteção do endpoint .
6.4.57	O Firewall deve conter, no mínimo, dois conjuntos de regras:	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico..
	a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; e	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	b) Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo,	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração de proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.

	protocolos poderão ser utilizados.	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.58	Capacidade de liberar acesso a um dispositivo externo por usuários e/ou grupo do AD (Active Directory), por período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;	Alterar	Capacidade de liberar acesso a um dispositivo externo por usuários e/ou grupo do AD (Active Directory), sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint .
6.4.61	Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);	Alterar	Capacidade de limitar a execução de aplicativos por nome do aplicativo e categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint .
6.4.62	Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há nenhum direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.4.63	Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web	Alterar	Em caso de epidemia o Endpoint deve ser capaz de se auto isolar de forma a não se proliferar pela rede.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint .
6.4.64	Capacidade de, caso o dispositivo de computação cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.	Alterar	Capacidade de manter as regras e proteções mesmo estando fora da corporação.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint .

6.5.2	Capacidade de instalação local e remota;	Alterar	Capacidade de instalação local	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint .
6.5.3	Deve possuir suportes a notificações utilizando o Growl	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.4	Capacidade de voltar para a base de dados de vacina anterior;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que fram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.5	Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.6	Possibilidade de desabilitar automaticamente varreduras agendadas quando o dispositivo de computação estiver funcionando a partir de baterias (notebooks);	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.10	Capacidade de agendar uma pausa na verificação;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.

6.5.11	O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
	6.5.11.1 Perguntar o que fazer, ou	Alterar	Submeter o arquivo suspeito automaticamente para análise de laboratório	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint.
	6.5.11.2 Bloquear acesso ao objeto;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.12.4	Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.13	Capacidade de verificar arquivos de formato de e-mail;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo, Mcafee e Kaspersky possuem o referido recurso tecnológico.
6.5.14	Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;	Retirar	Texto que sugere direcionamento a determinado fabricante.	Esta solicitação será atendida, ou seja, promoveremos a retirada desse item da Especificação Técnica para prover maior flexibilidade.

6.5.15	Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.	Retirar	Texto que sugere direcionamento a determinado fabricante.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração da proteção do endpoint e, não há direcionamento, visto que as duas últimas soluções que foram implantadas na PGE, devido a necessidade, como por exemplo Mcafee e Kaspersky possuem o referido recurso tecnológico.

GOVERNO DO ESTADO DO RIO DE JANEIRO
PROCURADORIA GERAL DO ESTADO

FORMULÁRIO PARA SUBMISSÃO DE SUGESTÕES

Nome do autor: *Add Value Participações, Comércio e Serviços de Informática Ltda.*

Endereço completo: *Rua Loefgren, nº 1057 – Conjuntos 501 a 503.*
Vila Clementino – Cep 04040-030 – São Paulo/SP

Forma de contato: 21 98493-9385 – geilson.melo@addvalue.com.br

Incluir item e nome do Documento (se possível, referenciar a folha)	**Contribuição** **(Deverá ser apresentada com a justificativa pertinente)**	**Resposta** **PGE-RJ**
6.1.3. Os softwares de antivírus deverão, no mínimo, prover Controle de Aplicações, **Firewall de host**, HIPS, IDS, Investigação (EDR), modulo para proteção de perda de dados (DLP) e Controle de Dispositivos integrados em único agente, gerenciado por uma única console;	6.1.3. Os softwares de antivírus deverão, no mínimo, prover Controle de Aplicações, HIPS, IDS, Investigação (EDR), modulo para proteção de perda de dados (DLP) e Controle de Dispositivos integrados em único agente, gerenciado por uma única console;	Não será atendida a solicitação de mudança de especificação técnica. Pois, reduz o escopo de proteção do endpoint.
6.1.11. Capacidade de instalar remotamente, automaticamente e em modo silencioso, para os dispositivos de computação (Windows, Linux);	6.1.11. Capacidade de instalar remotamente, automaticamente e em modo silencioso, para os dispositivos de computação (Windows);	Não será atendida a solicitação de mudança de especificação técnica. Pois, não atende completamente o ambiente heterogêneo da Rede da PGE.
6.2.2.1. Administração gráfica deve ser	Sugerimos o acréscimo da opção para que a solução de gerenciamento possa ser em nuvem, reforçando que os dados	Não será atendida a solicitação de mudança de especificação técnica. Pois, não há previsão de

acessada via WEB (HTTPS) e/ou através de uma Console Central de Gerenciamento, pode ser instalado em mais de uma máquina com acesso simultâneo	sensíveis a PGE-RJ, não ficam armazenadas nesse ambiente externo.	trabalhar com solução de nuvem na Rede PGE, por questão de segurança corporativa. Nos sistemas de nuvem, não há como determinar o local de armazenamento físico e tampouco quem irá acessar os dados.
6.2.2.38. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;	6.2.2.38. Aplicativos instalados, inclusive aplicativos de terceiros;	Este item irá permanecer da forma que esta especificado. É necessário que a solução seja abrangente com todas as opções solicitadas.
6.2.2.39. Informação completa de hardware e contendo: processadores, memórias, adaptadores, etc.;	Solicitamos a exclusão desse item, por entendermos que essas informações fogem ao escopo de uma solução de proteção a endpoints.	Esta solicitação será atendida, ou seja retiraremos esse item da Especificação Técnica por entender que poderá gerar limitação de competição.
6.2.2.55. Capacidade de ligar, desligar, reiniciar máquinas e também via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor	Solicitamos a exclusão desse item, já que entendemos que tais funcionalidades podem ser aplicadas ao sistema operacional.	Esta solicitação será atendida, ou seja, retiraremos esse item da Especificação Técnica por entender que poderá gerar limitação de competição.
6.4.3 -Antivírus de E-mail (verificação de e-mails recebidos e enviados, assim como seus anexos); compatibilidade com Exchange Active Sync;	Solicitamos a exclusão desse item, pois em nosso entendimento essas atividades estão relacionadas a soluções de borda	Esta solicitação será atendida, ou seja, retiraremos esse item da Especificação Técnica por entender que poderá gerar limitação de competição.
6.4.31 Até 6.4.43	Solicitamos a exclusão desse item, pois em nosso entendimento essas atividades estão relacionadas a soluções de borda	Esta solicitação será atendida, ou seja, retiraremos esse item da Especificação Técnica por entender que poderá gerar limitação de competição.
6.4.54 Deve ser possível bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group;	Solicitamos a exclusão desse item, pois em nosso entendimento essas atividades estão relacionadas a soluções de borda	Não será atendida a solicitação de mudança de especificação técnica. Pois, reduz o escopo de proteção do endpoint.

GOVERNO DO ESTADO DO RIO DE JANEIRO
PROCURADORIA GERAL DO ESTADO

FORMULÁRIO PARA SUBMISSÃO DE SUGESTÕES

Nome do autor: BRASOFTWARE INFORMATICA LTDA

Endereço completo: RUA MARINA LA REGINA, 277 – POÁ/SP

Forma de contato: MARCELA MENDES – MARCELA.MENDES@BRASOFTWARE.COM.BR 21 96431-6161

Incluir item e nome do Documento (se possível, referenciar a folha)	**Contribuição** **(Deverá ser apresentada com a justificativa pertinente)**	**ITEM**	**Resposta GTI-PGE.**
6.1.13	Sugerimos a remoção da palavra módulo. Pois a solução pode entregar essa funcionalidade, no entanto, não possui um módulo dedicado a isso.	As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições/assinaturas até o momento da expiração da licença;	Não foi identificado no item 6.1.13 a palavra "módulo".
6.1.8	Precisamos saber qual quantidade e os tipos de VMs que devemos considerar para o dimensionamento.	Deverá possuir solução contra a ação de ransomwares para (Servidores Virtuais) funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração e também proteção para os dados	No item Item 5 da Especificação Técnica está detalhado o quantitativo geral de licenças a serem adquiridas.

		compartilhados, bloquear o acesso do invasor ao compartilhamento e notificar o administrador.	
6.1.12	Retirar a premissa de remover automaticamente. Para antivirus terceiros, é necessário que a proteção de remoção esteja desabilitada e em determinados casos, a solução não estará na lista. Sendo necessário encaminhar para o suporte	Capacidade de remover automaticamente qualquer software de antivírus que estiver presente nos dispositivos de computação;	Entendemos que a solução deverá ser capaz de executar esta função automaticamente, portanto este item permanecerá como esta especificado no documento.
6.2	Recomendo a separação entre Servidor de Adm e Console Administrativa. Tendo em vista a compatibilidade diferente entre servidor e console.	**SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA**	Esta solicitação será atendida parcialmente. Promoveremos a alteração nesse item da Especificação Técnica a fim de aceitar as duas configurações, ou seja, centralizada ou separada.
6.2.1	O SERVIDOR Administrativo pode ser instalado apenas em SO Windows. Por isso se faz necessária a separaação dos itens Servidor de Administração e Console Administrativa. Além disso, cabe ressaltar que uma boa prática não instalar a console em diversos servidores.	**Compatibilidade** Mac OS X 10,12,13,14+; Red Hat Enterprise Linux Server 7x e superior (64Bits); CentOS Server 7x e superior (64Bits).	O servidor de administração poderá ser instalado no Windows, porém deverá ter compatibilidade com outros sistemas operacionais.
6.2.2.18	Retirar a premissa de remover automaticamente. Para antivirus terceiros, é necessário que a proteção de remoção esteja desabilitada e em determinados casos, a solução não estará na lista. Sendo necessário encaminhar para o suporte	Se possuir um antivírus diferente deverá remover automaticamente e instalar o novo.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para administração do endpoint.
6.3.2	Em relação ao serviço agentless é importante destacar dois pontos que precisam ser explicitados: (1) Se for AGENTLESS, é necessário saber a quantidade de CORES de cada processador (2) Se for com AGENTE é necessario saber a quantidade e o tipo de VMs que serão protegidas para servidores (WIN/LNX) e/ou estações (WIN/LNX).	Requer softwares corporativos de Antivírus especialmente otimizada para funcionar em conjunto com soluções de virtualização, por agentless ou contendo um agente otimizado e com requisitos reduzidos de recursos;	O Licenciamento especificado é por quantidade de dispositivo que o software de antivírus deverá ser instalado, independente se for VM/host fisico.
6.3.3	Como são licenças especificas é necessário	Deverá funcionar tanto em "Virtual	O item 5 trata da quantidade de licenças para

	informar a quantidade cada item: servidore e estação.	Servers" quanto em "Virtual Desktops";	servidores e estações, independente se for VM ou Hosts fisicos.
5.2	Comentário em relação a observação (forma de pagamento). Os fabricante dos softwares coorporativos de antivírus não possuem modelo de pagamento mensal. Sendo o pagamento efetuado em 30 após a entrega das licenças. As licenças são perpétuas.	Obs. Os valores pagos dos serviços de fornecimento e sustentação dos softwares serão parcelados em 36 vezes e os de implantação por unidade finalizada e aprovada pela Comissão de fiscalização.	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para a gestão do contrato na modalidade de serviço.
8.9.2	Sugerimos que seja desmenbrado o escopo do suporte do fabricande do suporte da contratada. Visto que o suporte do fabricante é atrelado as licenças. Já o suporte da Contratada está relacionado a mão de obra alocada, esta, podendo ser paga mensalmente.	Os serviços de manutenção preventiva e corretiva compreendem: a execução de aperfeiçoamentos e ajustes nas especificações originais, a correção de eventuais falhas de softwares que possam surgir durante a execução dos serviços, as aplicações de atualizações de produtos e serviços;	Não será atendida a solicitação de mudança de especificação técnica. Pois, é um requisito importante para a gestão do contrato na modalidade de serviço.

SUGESTÕES empresa STORBACK.

De: Luiz Fernando <luiz.fernando@storback.com.br>
Enviada em: sexta-feira, 14 de agosto de 2020 14:35
Para: Setor de Licitação PGE <licitacao@pge.rj.gov.br>
Cc: Erica Celeste <erica.celeste@storback.com.br>

Assunto: CONSULTA PÚBLICA PGE-RJ Nº. 04/2020 - Prestação de serviço de proteção corporativa de endpoint, incluindo a implantação, a sustentação e o fornecimento de softwares corporativos de antivírus com atualizações de versões.

Conforme a consulta pública PGE-RJ Nº. 04/2020, venho abaixo solicitar a revisão dos seguintes itens:

Referente ao Item:

5 – QUANTITATIVO DOS PRODUTOS, SUBITEM FORNECIMENTO E SUSTENTAÇÃO DOS SOFTWARES CORPORATIVOS DE ANTIVIRUS COM ATUALIZAÇÃO

Informamos que o fornecimento da solução (softwares/atualização), para a ferramenta que será disponibilizada ao órgão, não é possivel o parcelamento, somente o pagamento único, visto que são as melhores práticas do mercado.

*** Referente ao Item:**

6.1.3. Os softwares de antivírus deverão, no mínimo, prover Controle de Aplicações, Firewall de host, HIPS, IDS, Investigação (EDR), modulo para proteção de perda de dados (DLP) e Controle de Dispositivos integrados em único

No termo de referência não se faz nenhuma menção as funcionalidades de EDR e DLP, com isso fica muito vago o que o órgão pretende utilizar dessas ferramentas.

Para a solução de EDR**,** sugerimos a inclusão dos seguintes itens para identificar as funcionalidades:

1. EDR
1.1. A funcionalidade de EDR e cliente de antivírus devem ser integradas em um único agente, não havendo a necessidade de instalar mais de um componente no endpoint;
1.2. A ferramenta de EDR deve fazer detecção através do comportamento;
1.3. Deve fazer o correlacionamento de eventos entre computadores na rede (IoC Scanning);
1.4. Deve detectar elevação de privilégio;
1.5. Deve enviar objetos para verificação no Sandbox de forma automática quando necessário utilizando a inteligência global da fabricante;
1.6. Deve enviar objetos para verificação em Sandbox de forma manual;
1.7. O EDR deve permitir coletar informações forenses do endpoint tais como:
1.7.1. Dados;
1.7.2. Dumps de memória;
1.7.3. Estado do sistema operacional;
1.7.4. Processos iniciados;

1.7.5. Conexões estabelecidas;
1.7.6. Arquivos criados;
1.7.7. Registro modificado;
1.7.8. Tentativas de conexão com um host remoto;
1.7.9. Tentativa de login com sucesso;
1.7.10. Tentativa de login com falha;

1.8. Para segurança entre a comunicação entre o EDR e a Console de gerenciamento um certificado deve ser utilizado;

1.9. O EDR deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades abaixo:

1.9.1. Parar um processo;
1.9.2. Deletar um objeto;
1.9.3. Quarentenar um arquivo;
1.9.4. Recuperar um arquivo;
1.9.5. Prevenir a execução de um arquivo;
1.9.6. Executar um script;
1.9.7. Isolar o host completamente e de forma granular;

Para a solução de DLP, temos duas sugestões:

1) Retira-lo do item. Entendemos que a solução de DLP deveria ser um projeto a ser tratada de uma forma separada da solução de antivírus/endpoint, pois possui dimensões e requisitos mais robustos e dependem de um ambiente tecnológico aderente com detalhes que comummente não são contemplados em um projeto de antiviris/endpoint.

2) Especificar com mais detalhes o que é desejado dessa feature nas especificações do Termo de referência. Nossa ferramenta atende aos seguintes requisitos sem a necessidade de inclusão de uma solução especifica para o DLP:

i. DLP

1. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
    a. Discos de armazenamento locais;
    b. Armazenamento removível;
    c. Impressoras;
    d. CD/DVD;
    e. Drives de disquete;
    f. Modems;
    g. Dispositivos de fita;
    h. Dispositivos multifuncionais;
    i. Leitores de smart card;
    j. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
    k. Wi-Fi;
    l. Adaptadores de rede externos;
    m. Dispositivos MP3 ou smartphones;
    n. Dispositivos Bluetooth;
    o. Câmeras e Scanners.

2. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
3. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
4. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
5. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.
6. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

RESPOSTA GTI - PGE: Após análise das considerações apresentadas e entender a pertinência, iremos retirar o módulo DLP e, o modulo EDR será melhor detalhado conforme sugestão, na especificação técnica.

*Outro ponto a ser verificado, que, pelo conhecimento da ferramenta atual de antivírus utilizada pelo orgão, algumas features não estão sendo contempladas no termo de referencia, com isso, algumas funcionalidades que utilizam serão perdidas. Indicamos que seja incluído no termo referencia as seguintes funcionalidades que já possuem atualmente:

RESPOSTA GTI - PGE: Essa especificação não abrangerá a solução para dispositivos móveis.

1. **Gerenciamento de dispositivos móveis (MDM)**

1.1 Compatibilidade:

1.2 Dispositivos com os sistemas operacionais:

1.2.1 Android 5.0 – 5.1.1

1.2.1.1 Android 6.0 – 6.0.1

1.2.1.2 Android 7.0 – 7.12

1.2.1.3 Android 8.0 – 8.1

1.2.1.4 Android 9.0

1.2.1.5 Android 10.0

1.2.1.6 iOS 10.0 – 10.3.3

1.2.1.7 iOS 11.0 – 11.3

1.2.1.8 iOS 12.0

1.2.1.9 iOS 13.0;

1.2.2 Softwares de gerência de dispositivos:

1.2.2.1 VMWare Workspace ONE UEM 1905;

1.2.2.2 MobileIron 10.1 ou superior;

1.2.2.3 IBM Maas360 10.74 ou superior;

1.2.2.4 SOTI MobiControl 14.4 ou superior;

1.3 Características:

1.3.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

1.3.2 Capacidade de ajustar as configurações de:

1.3.2.1 Sincronização de e-mail;

1.3.2.2 Uso de aplicativos;

1.3.2.3 Senha do usuário;

1.3.2.4 Criptografia de dados;

1.3.2.5 Conexão de mídia removível.

1.3.3 Capacidade de instalar certificados digitais em dispositivos móveis;

1.3.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS;

1.3.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

1.3.6 Capacidade de, remotamente, bloquear um dispositivo iOS;

1.3.7 Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

1.3.8 Permitir sincronização com perfil do “Touch Down”;

1.3.9 Capacidade de desinstalar remotamente o antivírus do dispositivo;

1.3.10 Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

1.3.11 Capacidade de sincronizar com Samsung Knox;

1.3.12 Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

RESPOSTA GTI- PGE: A decisão da PGE é não incluir nesta contratação a solução para criptografia.

2 Criptografia

2.1 Compatibilidade

2.1.1 Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

2.1.2 Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

2.1.3 Microsoft Windows 7 Professional SP1 ou superior x86/x64;

2.1.4 Microsoft Windows 8 Enterprise x86/x64;

2.1.5 Microsoft Windows 8 Pro x86/x64;

2.1.6 Microsoft Windows 8.1 Pro x86/x64;

2.1.7 Microsoft Windows 8.1 Enterprise x86/x64;

2.1.8 Microsoft Windows 10 Enterprise x86/x64;

2.1.9 Microsoft Windows 10 Pro x86/x64;

2.2 Características

2.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

2.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

2.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

2.2.4 Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

2.2.5 Permitir criar vários usuários de autenticação pré-boot;

2.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

2.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

2.2.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

2.2.7.2 Criptografar todos os arquivos individualmente;

2.2.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

2.2.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

2.2.8 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

2.2.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

2.2.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

2.2.11 Verifica compatibilidade de hardware antes de aplicar a criptografia;

2.2.12 Possibilita estabelecer parâmetros para a senha de criptografia;

2.2.13 Bloqueia o reuso de senhas;

2.2.14 Bloqueia a senha após um número de tentativas pré-estabelecidas;

2.2.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

2.2.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

2.2.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

2.2.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

2.2.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

2.2.20 Permite criar um grupo de extensões de arquivos a serem criptografados;

2.2.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

2.2.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

2.2.23 Capacidade de deletar arquivos de forma segura após a criptografia;

2.2.24 Capacidade de criptografar somente o espaço em disco utilizado;

2.2.25 Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

2.2.26 Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

2.2.27 Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

2.2.28 Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

2.2.29 Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

2.2.30 Capacidade de fazer “Hardware encryption”;

RESPOSTA GTI - PGE: A decisão da PGE é não incluir nesta contratação a solução de gerenciamento de Sistemas.

3 Gerenciamento de Sistemas

3.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;

3.2 Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

3.3 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

3.4 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

3.5 Capacidade de gerenciar licenças de softwares de terceiros;

3.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

3.7 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;

3.8 Possibilita fazer distribuição de software de forma manual e agendada;

3.9 Suporta modo de instalação silenciosa;

3.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

3.11 Possibilita fazer a distribuição através de agentes de atualização;

3.12 Utiliza tecnologia multicast para evitar tráfego na rede;

3.13 Possibilita criar um inventário centralizado de imagens;

3.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

3.15 Suporte a WakeOnLan para deploy de imagens;

3.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

3.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

3.18 Capacidade de gerar relatórios de vulnerabilidades e patches;

3.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

3.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

3.21 Permite baixar atualizações para o computador sem efetuar a instalação;

3.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

3.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

3.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

3.25 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

3.26 Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

3.27 Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

3.28 Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

3.29 Deve permitir selecionar o idioma das aplicações que serão atualizadas;

3.30 Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;