DIÁRIO OFICIAL
Estado do Rio Grande do Sul

SECRETARIA DE PLANEJAMENTO, GOVERNANÇA E GESTÃO

RESOLUÇÕES

Gabinete do Secretário

RESOLUÇÃO

Resolução CGTIC Nº 02/2022

Regulamenta o uso da Solução Transversal de Antivírus do Estado do Rio Grande do Sul

O Comitê de Governança de Tecnologia da Informação, Comunicação e Inovação - CGTIC, no uso de suas atribuições conferidas pelo Decreto Estadual n° 56.106, de 24 de setembro de 2021:

RESOLVE:

I- No âmbito do Poder Executivo Estadual, abrangendo os órgãos submetidos à Política de TIC RS, quais sejam, a administração direta, as autarquias e fundações, estabelecer a Solução Transversal de Antivírus, como padrão de Segurança da Informação para *endpoints* .

II- Cabe ao Comitê Executivo de TIC implementar e monitorar esta resolução conforme os Anexos que seguem.

III- Entende-se *endpoint* como qualquer dispositivo conectado a uma rede de computadores, podendo ser desde servidores, computadores, notebooks, smartphones e laptops.

ANEXO I

Art. 1º A solução Transversal de Antivírus do Estado do Rio Grande do Sul é composta pelos componentes a seguir:

I - serviço de Gestão de Segurança da Infraestrutura de Antivírus - AVR da PROCERGS;

II- serviço de Diretório Ativo - ADS da PROCERGS; e

II- ferramenta de Antivírus/Endpoint padrão com Ata de Registro de Preços - ARP vigente.

Art. 2º A Solução Transversal será padrão no âmbito da administração pública estadual direta, autárquica e fundacional.

Art. 3º O Serviço AVR é transversal e consiste no conjunto de serviços e infraestrutura que possibilitam a Gestão do ambiente centralizado e o controle e suporte administrativo às licenças de Antivírus para o Estado, contemplando os seguintes processos:

I- gestão do ambiente;

II- suporte técnico;

III- administração de licenças;

IV- consultoria e assessoria em projetos de implantação; e

V- migração e parametrização dos produtos contemplados no contrato para uso da solução de antivírus constante da

ARP vigente.

Art. 4º O Serviço ADS é transversal e consiste em um diretório usado para armazenar informações sobre os recursos tecnológicos, como microcomputadores e impressoras, assim como os usuários individuais e grupos, disponíveis na rede de comunicação do Órgão, contemplando os seguintes processos:

I- implantação do ambiente; e

II- manutenção do ambiente operacional e monitoração do serviço;

Art. 5º A Ferramenta de Antivirus/Endpoint padrão, aprovada pelo CETIC e com ARP vigente poderá, ao final do respectivo contrato, ser alterada conforme análise de custo.

Art. 6º Os órgãos e as entidades estaduais não deverão adotar padrão próprio de gestão de Antivírus, salvo prévia autorização do CETIC, que analisará os riscos e as comprovações de capacidade técnica para instalar, manter e gerenciar uma solução tecnicamente equivalente e compatível com os níveis de riscos aceitos na solução transversal do Estado.

§ 1º A excepcionalização deverá ser revogada quando deixarem de existir as condições mínimas exigidas.

§ 2º OS Anexos II a IV, desta resolução, determinarão os critérios mínimos e recomendados para excepcionalização.

ANEXO II

Requisitos Mínimos para Gestão de Segurança da Infraestrutura de Antivírus

Requisito	**Mínimo e Obrigatório**	**Desejável**
Requisitos mínimos de Hardware:		
Infraestrutura de Hardware e software mínimos necessários para rodar a ferramenta de antivírus/endpoint conforme definido na documentação do fornecedor da solução contratada, podendo ser *on-premise* (local) ou *cloud* (nuvem).	**x**	
Requisitos mínimos de Equipe:		
Equipe de TI com no mínimo duas pessoas, não necessariamente dedicadas.	**x**	
Requisitos mínimos da Administração Técnica do Contrato		
Acompanhamento junto ao Fornecedor de: Ateste de Faturas, acompanhamento de SLAs, acompanhar a disponibilidade dos serviços e controle de Licenças;	**x**	
Disponibilização, sob demanda do Sistema de Governança e Gestão de TIC, de relatórios de segurança e gerenciais;	**x**	
Acompanhamento e implementação das Políticas de Segurança instituídas pelo Sistema de Governança e Gestão de TIC	**x**	
Controle de vigência e renovação dos contratos para que não haja descontinuidade dos serviços."	**x**	
Requisitos mínimosde Gestão:		
Gerenciamento de licenças de software de proteção de endpoint (antivírus):		

Deve haver processos e ferramentas de controle e documentação das licenças de software de proteção de endpoint utilizado. Deve controlar o uso das licenças dentro do número e prazo adquirido junto ao fornecedor	**x**	
Gestão de incidentes		
Aplicação de conjunto de boas práticas que visam a manutenção, operação e infraestrutura dos serviços de TI e capacidade de restaurar a operação normal do serviço o mais rápido possível	**x**	
Gestão de vulnerabilidades		
Capacidade de identificar, notificar, analisar e corrigir de forma contínua as vulnerabilidades identificadas.	**x**	
Gestão de riscos		
Consiste no conjunto de boas práticas que visamidentificar, avaliar e priorizar riscos, seguido da aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável	**x**	
Gestão de políticas		
Capacidade de identificar, monitorar e implementar as normativas e regras de Segurança estabelecidas em nível de Estado e da Organização	**x**	
Monitoramento do ambiente		
Capacidade de visualizar os eventos técnicos que podem levar a um incidente. Consiste em processo automatizado de recebimento, análise e armazenamento de dados enviados por equipamentos de segurança eletrônica. Consiste na capacidade de utilização dos recursos tecnológicos empregados para prevenir que os ativos importantes do órgão sejam acessados e explorados indevidamente.	**x**	
Treinamento com o fornecedor da solução		
A equipe de TI, responsável pela operação dos sistemas, deverá estar capacitada para o uso pleno das ferramentas de segurança contratadas	**x**	

ANEXO III

Requisitos Mínimos para Diretório Ativo (*ActiveDirectory)* próprio

Requisito	Mínimo e Obrigatório	Desejável
Servidores Controladores de Domínio (*DomainControllers*)		
No mínimo 2 (dois) servidores (físicos ou virtual) exercendo a função controladores de domínios, ambos com a função de *Global Catalog* ativas independentemente de estarem ou não no mesmo site, garantindo assim a disponibilidade mínima dos serviços de diretório;	**x**	
***Local Administrator Password Solution* (LAPS) - Microsoft**:		
Deve estar instalado, configurado e habilitado por default no domínio, aplicado a todos os servidores membros e estações de trabalho. O LAPS como solução de gestão e controle de identidade de usuários local, auxilia a gestão de segurança na prevenção contra ataques laterais comumente causados por malwares, como ransomware, por exemplo;	**x**	
Políticas de grupo (*GroupPolicy*) - GPO:		
Devem estar aplicadas aos domínios políticas que auxiliem na confidencialidade, integridade e disponibilidade do ambiente, configuradas e aplicadas preferencialmente baseadas no conceito de Zero Trust, entre elas:	**x**	
Firewall : Política para controle de Firewall (padrão ativado) com exceção apenas para portas necessárias para funcionamento de aplicações, com a devida justificativa registrada junto a equipe de administração do domínio, bem como a de segurança da informação, sendo as exceções de inteira responsabilidade do solicitante autorizado;	**x**	
Grupos Restritos : Política de uso de grupos restritos para controle de acesso administrativo em servidores membros e estações do domínio;	**x**	
Proxy : Política de Proxy habilita a todos os usuários do domínio, sendo os casos de exceção devidamente registrados junto a equipe de administração do domínio, bem como a de segurança da informação, sendo as ações executadas pós concessão, de inteira responsabilidade do solicitante autorizado;	**x**	

Acesso Remoto: Políticas de acesso remoto configurada e aplicadas a todos os servidores membros e estações de trabalho do domínio, sendo a definição dos grupos e/ou usuários autorizados definidamente registrada pelos administradores de domínio, bem como a equipe de segurança da informação;	**x**	
Auditoria : Deve estar habilitada no mínimo os seguintes tipos de auditoria via *policy* : Eventos de *logon* , gerenciamento de contas, acesso ao serviço de diretório, acesso a objetos, mudança de diretivas, uso de privilégios e eventos do sistema;	**x**	
Windows Updates : Políticas de grupo para fins de aplicação de updates para *domaincontrollers,* servidores membros e estações, devidamente configuradas e habilitadas, preferencialmente apontadas para um servidor WSUS, caso não possível, ao menos para o Windows Update;	**x**	
Autorun : Política para bloqueio de*autorun* em servidores e estações.		
Gestão de usuários e grupos :		
Limitar os integrantes dos grupos administrativos Built-inDomainAdmins, Administrators, DNSAdmins, Backup Operators, etc, somente os usuários diretamente envolvidos na gestão e administração do domínio, evitando sempre o uso de contas de serviço. As atividades relativas a operação do domínio devem estar separadas e autorizadas por concessão de delegação de controle a grupos específicos e devidamente catalogados junto a administração do domínio e equipe de segurança da informação. Casos de exceção são de responsabilidade direta do solicitante e/ou autorizado;	**x**	
Ativos :		
Para fins de melhor gerenciamento e monitoramento, todos os ativos considerados servidores membros e estações de trabalho, deverão serem ingressados no domínio, inclusive aqueles com Sistema Operacional não Microsoft, como os Linux e MacOS, por exemplo, não cabendo exceção visto que hoje em dia todos os sistemas tem compatibilidade e interoperabilidade com os serviços de diretório Microsoft, seja através de pacotes em repositórios oficiais ou nativo nos Sistemas Operacionais	**x**	

ANEXO IV

Requisitos mínimos para Ferramenta de Antivírus

Requisito	Mínimo e obrigatório	Desejável
Software		
O software de proteção deve compreender as seguintes funcionalidades: Prevenção de ameaças; Firewall e prevenção contra intrusão; Prevenção adaptável contra ameaças	**X**	
A proteção deverá conter um agente de gerenciamento independente dos softwares de proteção, permitindo que componentes sejam adicionados ou removidos conforme às necessidades dos administradores	**X**	
O conjunto de softwares de proteção e agente de gerenciamento deverão ser fornecidos pelo mesmo fabricante	**X**	
Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de: Monitoramento de eventos; Relatórios; Dashboards; Políticas; Configuração; Atualizações de vacinas e de software; Instalação/Desinstalação;	**X**	
A solução deve possuir integração com SIEM, fornecendo logs para o correlacionar de eventos de segurança		**x**
O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente	**X**	
O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante	**X**	
A comunicação entre o cliente gerenciado e o servidor de gerenciamento central deverá ser autenticada por um par de chaves para garantir a identidade das partes	**x**	
A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise contextual, não baseada somente em assinaturas de detecção	**X**	
A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas	**X**	

O agente cliente deve enviar para o servidor de gerenciamento central informações sobre o cliente gerenciado incluindo, pelo menos, as seguintes: Endereço MAC, IP, Endereço da Subrede e Máscara; Nome de DNS e Domínio; Sistema Operacional, tipo e versão; Produtos da solução antimalware instalados no sistema; Nome ou Login do usuário	**x**	
A solução deverá realizar verificações periódicas no ambiente para alertar o fabricante de potenciais problemas ocasionados pela atualização de vacina	**X**	
A solução deve conter módulo capaz de proteger contra redes de BOT, negação de serviço, executáveis não confiáveis e conexões web maliciosas	**X**	
O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede	**x**	
A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)		**X**
A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre soluções de fabricantes terceiros (Exemplo: Checkpoint, Fortinet, Avecto, TrapX, Fireeye, NMAP, Cisco, IBM), compartilhando as informações para melhor mitigar novas ameaças		**X**
Ativos:		
Para fins de melhor gerenciamento e monitoramento, todos os ativos considerados endpoints, deverão possuir programa de antivírus instalada e serem inseridas no gerenciador centralizado, inclusive aqueles com Sistema Operacional não Microsoft, como os Linux e MacOS, por exemplo, não cabendo exceção	**x**	

CLAUDIO GASTAL
Av. Borges de Medeiros, 1501, 2º andar
Porto Alegre
CLAUDIO GASTAL
Secretário de Planejamento, Governança e Gestão
Av. Borges de Medeiros, 1501, 2º andar
Porto Alegre
Fone: 5132881200

Publicado no Caderno do Governo (DOE) do Rio Grande do Sul
Em 6 de Outubro de 2022

Protocolo: **2022000778287**

Publicado a partir da página: **69**