



### ATA DE REUNIÃO

<b>Data:</b> 25/11/2021	<b>Início:</b> 10:00	<b>Fim:</b> 10:35
<b>Local:</b> Sala da Coordenação-Geral de Modernização e de Tecnologia da Informação		
<b>Pauta:</b> 1. Levantamento técnico de informações da solução de DLP para a Funasa		

### PARTICIPANTES

Nome	E-mail	Unidade
André Wilson Pimenta Santana	<a href="mailto:andre.pimenta@funasa.gov.br">andre.pimenta@funasa.gov.br</a>	COINT
Silvano José de Souza	<a href="mailto:silvano.souza@funasa.gov.br">silvano.souza@funasa.gov.br</a>	COINT
Alexander Bastos	<a href="mailto:alexander.bastos@broadcom.com">alexander.bastos@broadcom.com</a>	SYMANTEC

### PONTOS DISCUTIDOS

Resumo
<ol style="list-style-type: none"><li>Alexander (Symantec) inicia a reunião apresentando as licenças que a coordenação tem, e que são licenças perpetuas, e dependendo de como for o projeto irá conseguir reativar todas essas licenças, para fazer o processo com confecção.</li><li>Alexander (Symantec) segue informando que existem pacotes ou verticais de solução, por exemplo: o DLP é uma vertical de solução, você não consegue renovar um pedaço do DLP, e sim ele inteiro. A proteção do endpoint e EDR, tudo junto, e essa também ele completou afirmando que não consegue separar, mas se for dentro dessas verticais é possível que consiga, e pode ter a opção de escolher renovar apenas um contrato dos sistemas, ou seja, se preferir renovar apenas um e os outros não tem problema.</li><li>Alexander (Symantec): Pergunta ao André o que ele de fato precisa para adquirir na gestão, e que antes a gestão de TI tinha uma suíte completa de DLP, essa suíte completa de DLP já está defasada, ela já não é mais totalmente completa. Alexander pontua que no pacote que ele oferece tem módulos de rede, moldes de cloud, solução de casb, tudo dentro do módulo de DLP nuvem, e que tudo é incluso em um pacote, por isso a importância de saber o que o André está necessitando no ambiente da gestão para poder fornecê-lo, e completa que o que a gestão tinha já configurado estava em um grau de maturidade muito bom, era um dos lugares em Brasília que tinha um grau de maturidade de implementação de DLP mais avançado, e implementar novamente seria rápido e eficaz, e como a gerência de DLP é uma gerência única, todo esse trabalho de política, ele automaticamente consegue ser distribuído para todos os modos em nuvem.</li><li>Silvano (coint): Silvano informa que não sabe ao exato como está a situação do DLP atual, mas que não teve problema até então.</li><li>Alexander (Symantec): completa que se não teve problema, é só fazer um ressaltos para voltar a ter tudo que tinha. Completa que pelo que a empresa tem visto, a solução em nuvem tem sido muito efetiva, pelo fato de ter bastante configurações, e certas coisas davam muito trabalho para serem executadas. Já a de nuvem trabalha com uma maneira muito mais na linha da inteligência artificial, então o nível de categorização e de identificação do spam tem sido um nível bem elevado.</li></ol>

6. Alexander (Symantec): questiona que o trabalho administrativo do André irá dobrar, porque uma informação quando ela caminha dentro do seu ambiente, ela não irá monogamicamente, ela irá para nuvem também. Toda vez que fizer uma política, o seu próprio administrador vai ter que se lembrar de fazer uma política diretamente para a nuvem, se ele não replicar para dentro da nuvem terá uma grande chance de falha e com risco de vazamento dentro de casa. Apesar do ambiente de DLP estar em nuvem, quem acessa o ambiente é o desktop de dentro de casa, seja ele dentro da Funasa, ou dentro da casa do colaborador, então o DLP desse desktop é um DLP on-premise, se você fizer uma política aqui, na hora que a informação for, pode ter risco de vazamento na hora que quiser, ou se a máquina do usuário tiver atacada, como você não está utilizando Symantec, a solução de DLP impede a informação e não o desktop. O DLP trava esse envio de informação, à grosso modo, ao primeiro check, a partir da autenticação do usuário quando você vai fazer uma barra barra, como por exemplo, um servidor de arquivo, primeiro você faz a sua autenticação como usuário você finaliza e salva o arquivo. Isso acontece em todas as aplicações de dentro da máquina, se a sua máquina for afetada na hora que esse aplicativo que foi atacado for tentar estratificar o dado ele vai tentar estratificar com a sua credencial, o DLP não tem inteligência para detectar que aquele processo é um processo malicioso, ele vai verificar que aquele processo está autorizado pelo usuário, a informação irá vazamento. Então quando nós falamos sobre DLP o ideal é fazer em uma única solução, nem que faça em momentos distintos, mas que você tenha um único fabricante, não importa qual, mas por segurança seria aconselhado apenas um. A quantidade de incidentes que um DLP mal configurado te entrega, você vai desistir do produto, qualquer evento que a política está mal configurada ele alarma uns 500 milhões de uma vez só.
7. Alexander prossegue informado que aconselha fazer essa atualização, a montar o ambiente novo, com modelo de poc, ou modelo de ata, levantar todo ambiente com a versão atual e já vai trabalhando na versão de nuvem, fazer um poc de 4, 5 ou 6 meses.
8. André (coordenador): complementa que quando for desenhar o ETP tem que buscar outras soluções no mercado até para demonstrar e ver qual é a melhor solução.
9. Alexander (Symantec): solicita uma estimativa de quantitativo de usuários, André responde que atualmente tem 3.190 usuários.
10. Alexander (Symantec): informa que precisa de um número de usuário local para ele habilitar a energia internamente, se mais na frente tiver uma licença de 100 usuários e o órgão está utilizando 300, mas os 300 estão contemplados nesta conta da nuvem, só necessitará do número para habilitar os dois ambientes.
11. Silvano (coint): responde para Alexander que serão 3.500 usuários, pelo fato do fluxo que aumenta e diminui no decorrer do tempo, mas que para o DLP continua o quantitativo de 3.190 usuários.
12. Alexander (Symantec): finaliza que precisa de um comunicado de qual caminho estará subindo e que tem autorização para subir todo o ambiente e solicitar um engenheiro para a execução do sistema, sem custo, com todas as soluções na última versão, tentar fazer aos poucos as migrações e um parceiro para trabalhar junto com o órgão.
13. André (coordenador): finaliza a reunião agradecendo a apresentação de Alexander e informa que irá pesquisar outros fabricantes, para levantar todos os valores, e fazer os ajustes que precisar para instruir o processo da melhor forma possível.