Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE

doi.org/10.51891/rease.v8i12.8081

O USO DE VIRTUALIZAÇÕES EM CONTEINERS COM O DOCKER PARA ALEI GERAL DE PROTEÇÃO DE DADOS

GENERAL DATA PROTECTION LAW AND COMPUTER ENGINEERING PERFORMANCE

Jonathas Barros Ferreira[1]
Edilson Carlos Silva Lima[2]

RESUMO: O fluxo do volume de informações cresceu através do rádio, televisão, cinema e telefone. Haja vista que os dados se encontram na esfera virtual,incluindo imagens, vídeos e mensagens, a privacidade dos indivíduos pode ser lesada. Sancionada em 14 de agosto de 2018 pelo então presidente Michel Temer,a Lei nº 13.709, denominada Lei Geral de Proteção de Dados, a qual envolveu extraordinariamente o tema e editou dispositivos do Marco Civil da Internet. No entanto, apesar da importância da Lei em questão, afirma-se que persistem diversas omissões quanto à proteção de dados, o que afeta de forma significativa a sociedade informacional. A virtualização é uma maneira segura de garantir otimização no uso do hardware, a exemplo que iremos usar neste artigo, o docker,que usa contêiners para simular recursos de outro sistema, trazendo otimização degerenciamento, redução de custos. Foi realizado um estudo de caso a partir de pesquisas bibliográficas de uma empresa chamada ME, na qual precisa ter os documentos organizados e protegidos para não ter nenhuma violação, acesso indevido dessa forma criado uma máquina virtual no virtual box.

Palavras-chave: Conteiners. Virtualização. Docker. LGPD.

ABSTRACT. The flow of information grew through radio, television, cinema and telephone. Given that data is in the virtual sphere, including images, videos and messages, the privacy of individuals can be harmed. Enacted on August 14, 2018by the then President Michel Temer, Law No. Fundamental to citizens who providetheir data in the digital environment. However, despite the importance of the Lawin question, it is stated that several omissions regarding data protection persist, which significantly affects the informational society. Virtualization is a safe way to ensure optimization in hardware usage, as we will use in this article, docker, which uses containers to simulate resources from another system, bringing management optimization, cost reduction. A case study was conducted frombibliographic research from a company called ME, in which you need to have thedocuments organized and protected to have no violation, misused access in this way created a virtual machine in the virtual box.

Keywords: Conteiners. Virtualization. Docker. LGPD.

[1] Engenharia de Computação – Universidade Ceuma (UniCEUMA) – Cidade São Luís – MA – Brasil.
[2] Engenharia de Computação – Universidade Ceuma (UniCEUMA) – Cidade São Luís – MA – Brasil. Marcos José dos Passos Sá.

1. INTRODUÇÃO

O presente artigo se prendeu a fontes bibliográficas partindo disso, a pesquisa se constitui em demonstrar a segurança em um setor de RH, da empresa fictícia que neste artigo será chamada de ME, onde se tem 6 (seis) funcionários, os mesmos tem perfil de acesso a pasta de documentos compartilhados, a pasta chamada de funcionários, onde os mesmos estão fazendo *upload* dos arquivos pdf, txt, dentro da pasta compartilhada pertencente ao RH. Para fazer a segurança e solucionar o problema foi criada uma máquinavirtual no *software* Virtual Box. Os arquivos do RH ficam restritos ao seu setor sem interferências de outros setores e com a assinatura digital impedindo de pessoas dos demais setores de acessar, reescrever.

Atualmente, o próprio indivíduo fornece, irresponsavelmente, suas informações e,às vezes exigidas legitimamente, a terceiros, disfarçado de cadastros, assinaturas ou aindade pesquisas de opinião, nas quais, ao término, é requerida a comunicação de dados pessoais para "validação" da resposta. Isto posto, em um panorama contextualizado, o atualparadigma da privacidade não deve se limita aos ilícitos de outrora, deve englobar ainda osatuais. Conforme Fortes (2016):

> Em perspectiva histórica mais recente, são identificadas duas maneiras deviolação de privacidade. A primeira consiste na coleta de informações pessoais ea segunda concentra-se no seu uso. O primeiro modo de violação da privacidadepode ser realizado de dois modos: ilícito, quando clandestinamente, alguém coletainformações pessoais, a fim de descobrir aquelas que ainda não se tornaram públicas; lícito quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa.

A vulnerabilidade pode ser extrínseca, isto é, a possibilidade de a empresa ser acometida por ataques de terceiros, ou intrínseca, proveniente de atitudes dos próprios colaboradores. Segundo a Lei Geral de Proteção de Dados, na hipótese de incidente de segurança, devem ser notificados à Autoridade Nacional de Proteção de Dados e o titular dos dados expostos. Por incidente de segurança, entende-se qualquer evento indesejado ou imprevisto, confirmado ou sujeito a confirmação, passível de lesar a segurança de dados pessoais, sendo de maior amplitude em relação ao vazamento de dados, que constitui somente uma das hipóteses de incidente de segurança. (BRASIL, 2018).

Uma ferramenta importante para a proteção de dados é o docker, o docker é um container de uma unidade padrão de software que empacota o código e todas as suas

dependências para que o aplicativo seja executado de forma rápida e confiável. Uma imagem de contêiner do Docker é um pacote de software leve, autônomo e executável queinclui tudo o que é necessário para executar o aplicativo: código, tempo de execução, ferramentas do sistema, bibliotecas do sistema e configurações. Os contêineres isolam o software de seu ambiente e garantem que ele funcione uniformemente, apesar das diferenças. (DOCKER, 2022).

Neste artigo vamos abordar tópicos importantes, sendo eles: a fundamentação teórica metodológica no capítulo 2, no capítulo 3 discutiremos sobre o estudo de caso do assinador de arquivo usado dentro do docker, no capítulo 4 falaremos sobre os resultados ediscussões, e ao final as referências usadas para compor este artigo.

2. SOFTWARE USADOS NA LGPD

Neste capítulo vamos abordar uma revisão bibliográfica com um estudo de caso dos assuntos essenciais para a Lei Geral de Proteção de Dados e está dividido nos seguintesitens: 2.1 Virtualização, no item 2.2 Virtual Box, item 2.3 *Conteiners*, no item 2.4 *Docker*,item 2.5 Segurança em sistema distribuído.

2.1 Virtualização

A virtualização usa um software para criar uma camada de abstração sobre o hardware físico, essa é uma técnica de separar sistemas operacionais e aplicações dos componentes físicos, ao ser realizado isso, é criado um sistema de computação virtual, conhecido como máquina virtual. Estas máquinas virtuais permitem que organizações de vários computadores com seus sistemas e aplicativos funcionem como se fosse um servidorfísico, essa é uma forma muito eficaz de conseguir acesso a recursos sem prejudicar o sistema operacional e hardware instalado. (SHAMIRE, 2021).

Os benefícios da virtualização, se caracterizam pela redução de despesas com hardware, redução do tempo de inatividade e aumento da resiliência em casos de desastre quando afeta um servidor físico levando apenas alguns minutos para a recuperação, aumentoda eficiência e produtividade.

2.2 Virtual box

O virtual box é um software de virtualização, indicado para pessoas físicas ou jurídicas

de qualquer porte ou segmento, que tenham como objetivo um bom desempenho,voltado para servidores, desktops e uso integrado. Com este software instalado é possível executar vários sistemas operacionais ao mesmo tempo ou individualmente, sem precisar necessariamente instalar qualquer sistema operacional em seu dispositivo. Como exemplo pode ser executado ao mesmo tempo o Windows, Linux e Solaris ao mesmo tempo, tal combinação pode ser ajustada conforme a necessidade. (LIRA, 2021).

A sua utilização é gratuita, para todos os sistemas operacionais, Windows, Mac OS, Linux de 64 bits, sendo necessário espaço em disco, memória e um bom processamento de CPU. Ao criar uma máquina virtual, é possível configurar vários parâmetros como, definir nome de cada uma, criar perfil em nuvem, estipular número de núcleos de CPU virtuais de cada máquina. Alguns dos benefícios a longo e curto prazo, é a redução de custo de diferentes hardwares, redução com eletricidade, reduz servidores, otimização de espaço, os desenvolvedores podem realizar diversos testes em uma única máquina. (LIRA, 2021).

2.3 *Conteiners*

Uma das tecnologias mais populares que se tem atualmente é o uso de contêineres para a execução de sistemas dos mais variados tipos. Devido a sua facilidade e à flexibilidade, que acontecem do uso dos mesmos. O contêiner funciona como tecnologia dando suporte para o funcionamento de aplicações e pode ser considerado um emulador de uma aplicação. (PEREIRA, 2019).

A aplicação quando executada através de um contêiner, ela tem todas as bibliotecase os elementos necessários para o funcionamento disponíveis dentro deste contêiner. Uma maneira direta para entender contêiner é imaginar que eles permitem a criação de ambientes virtuais isolados e autônomos para serem utilizados por aplicações, similar ao resultado douso de máquinas virtuais. O seu grande diferencial está no fato de que os contêineres são mais leves que máquinas virtuais, por serem completamente otimizados. (PEREIRA, 2019).

2.4 *Docker*

A tecnologia de contêiner Docker foi criada e lançada no ano de 2013 como um *Docker Engine* de código aberto. O mesmo impulsionou os conceitos de computação existentes ao entorno de contêineres e espacialmente no nicho do Linux. A tecnologia do

Docker é única porque se aplica nos requisitos dos desenvolvedores e operadores de sistemas a fim de separar as dependências de aplicativos de infraestrutura. (DOCKER, 2022).

O docker, famosa plataforma genérica de conteinerização, sendo muito popular atualmente devido a flexibilidade que vêm de seu uso. (PEREIRA, 2019).

Sendo uma plataforma *open source* que facilita a criação e administração dos ambientes isolados, possibilitando o empacotamento de uma aplicação, ambiente dentro de um container, tornando-se portátil para qualquer outro host tendo a flexibilidade de migrar de um ambiente para o outro. A ideia principal do docker é subir uma máquina ao invés de várias tendo em uma única máquina várias aplicações sem que haja conflito entre as demais. (GUEDES, 2018).

2.5 Segurança em sistema distribuído

O sistema distribuído implementado tem como principal aspecto a segurança, no sistema distribuído temos uma série de componentes de hardware e software, físicos ou virtualizados onde se comunicam para execução das aplicações distribuídas. Uma forma funcional de prevenir é usar o sistema de segurança de multicamadas, na qual ela protege com diferentes tecnologias de segurança os principais pontos de ameaças. (CAIQUE, 2019).

A segurança utilizando multicamadas aumenta o grau de dificuldade para invasãode um invasor, diminuindo drasticamente o risco de um hacker ter acesso indevido à rede edados de uma empresa, colégio, bancos. Com esta estratégia de multicamadas, as ameaçasencontram uma maior dificuldade em causar dano, porque caso ultrapassem alguma camadadeverão ser barradas pela camada seguinte, quando implementada corretamente várias camadas ofererecerão proteção com o vírus.

Figura 1. Pilares da segurança da informação.

Fonte: Silveira, 2017.

Podemos relacionar a segurança de um sistema distribuído aos seguintes fatores: (PEREIRA, 2019).

3. Confidencialidade

A confidencialidade significa que a informação só estará disponível para osusuários ou máquinas autorizadas. Uma das formas de se garantir confidencialidade das mensagens é através do uso de autenticação baseada emchave privada.

4. Integridade

A integridade significa que a informação armazenada ou transferida é apresentada corretamente para quem precisa fazer a sua consulta. A integridade dasmensagens pode ser alcançada através de assinaturas digitais e chaves de sessão.

5. Autenticidade

A autenticidade pode ser alcançada quando criamos permissões de autenticação para os principais usuários e máquinas do serviço, com isso nosso sistema só irá funcionar corretamente com os usuários e máquinas autenticadas.

6. Disponibilidade

A disponibilidade significa garantir que a informação esteja sempre disponível para quem precisar dela. Podemos obter a disponibilidade do sistema utilizando as políticas de segurança corretamente em nosso sistema.

7. Não repúdio

O não repúdio ou princípio do não repúdio, como é conhecido, garante a autenticidade de uma informação utilizada por sistemas distribuídos. Ele é uma grande medida de segurança, já que pode ser aplicada a e-mails, imagens,formulários web, arquivos eletrônicos transferidos entre empresas (EDI), entreoutros itens. Uma das principais maneiras de se aplicar essa exigência de segurança é através de assinatura digital e certificados digitais.

8. A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Sancionada em 14 de agosto de 2018 pelo então presidente Michel Temer, a Lei nº 13.709, denominada Lei Geral de Proteção de Dados, a qual envolveu extraordinariamenteo tema e editou dispositivos do Marco Civil da Internet, representando um grande avanço para a garantia de direitos fundamentais aos cidadãos que fornecem seus dados no ambientedigital.

A importância e valia da discussão a respeito da proteção e dados pessoais pode ser bem esclarecida quando observadas empresas como Facebook e Google, duas das maiores empresas globalmente, em que grande parte dos lucros são oriundos de serviços gratuitos que coletam dados de seus usuários sendo empregados na prática da publicidade direcionada. O tema se revela de fundamental importância para titulares dos dados e empresas executoras do tratamento, garantindo ao usuário o seu direito de privacidade e a convicção do fim direcionado aos dos disponibilizados, tal como a possibilidade dasolicitação por parte do usuário de relatórios sobre o tratamento e armazenamento de seus dados.

Igualmente ao Marco Civil, a LGPD também instituiu termos técnicos relativos ao tema, visando equiparar a interpretação aos diferentes casos. Portanto, torna-se evidente o intuito da lei em tutelar a pessoa natural enquanto titular dos dados pessoais, não passível de valor à pessoa jurídica. Outrossim, constata-se que a Lei nº 13.709 não protege dados anônimos, esclarecendo que a concepção de dados pessoais requer a titularidade de uma pessoa natural identificável, destacando que na hipótese da reversão do anonimato, deve-setratá-lo, assim, como dado pessoal.

Anteriormente à LGPD, a coleta de dados era promovida indiscriminadamente, contudo, com o seu advento, passará a ser regulada, pois a Lei institui o modo pelo qual o tratamento, transferência e comercialização dos dados obtidos deve ser realizado. Com a LGPD, o direito à privacidade se torna o direito mais protegido, o que outrora eraassegurado na Constituição na era dos dados físicos, passa a ser garantido ainda no ambiente digital, acompanhando a tendência mundial relativa à proteção de dados pessoais, sobretudo a legislação europeia.

A Lei Federal nº 13.709, de 14 de agosto de 2018, aprovada pelo então presidente Michel Temer, está em vigor desde fevereiro de 2020, versando sobre vários aspectos que anteriormente não dispunham de previsão legal, ou cujo tratamento se dava de modo esparso em leis setoriais, sem uma unificação.

8.1 Como foi criado o Docker

Para que o docker possa ser executado antes de instalar é preciso remover suas versões antigas, as antigas versões do docker conhecidas como docker, docker.io, docker -engine. O seguinte comando foi utilizado para que estas versões citadas acima fossem retiradas:

$ sudo apt-get remove docker docker-engine docker.io containerd runc

Se for retornado uma mensagem avisando que nenhum dos pacotes acima está instalado, isto ocorre porque imagens, contêiners, volumes não são removidos quando se desinstala o docker, nesse caso deve-se seguir outro método que não será abordado aqui neste artigo, mas em caso de dúvida todas as informações encontram-se no site oficial do Dokcer.

Em seguida, foi atualizado o índice de pacotes e instalados para que fosse permitidoo uso do repositório por *HTTPS*, cada comando foi executado separadamente e obedecendoas quebras de linhas necessárias, primeiro foi utilizado o comando:

$ sudo apt-get update $ sudo apt-get install \ca-certificates \ curl \ gnupg \ lsb-release

Foi adicionado a chave oficial do Docker:

$ sudo mkdir -p /etc/apt/keyrings $ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg

Configurado o repositório usando o comando:

$ echo \ "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu \ $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

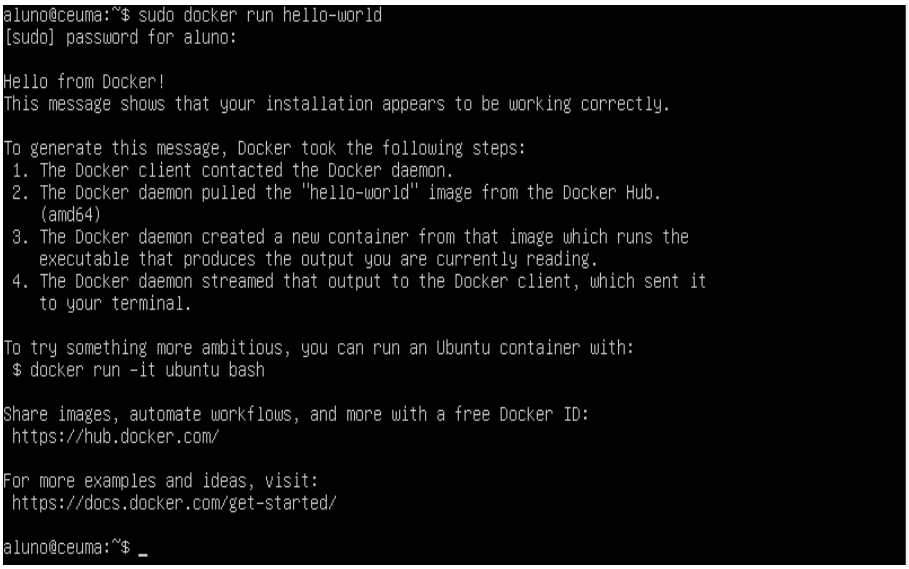
Em seguida foi feita a execução do Docker para que o serviço fosse iniciado

$ sudo service docker start

Verificou-se se a instalação foi bem sucedida com dois comandos, o primeiro uma imagem, o segundo verificando se os serviços estão ativos.

$ sudo docker run hello-world

Figura 2. Comando Hello-World.



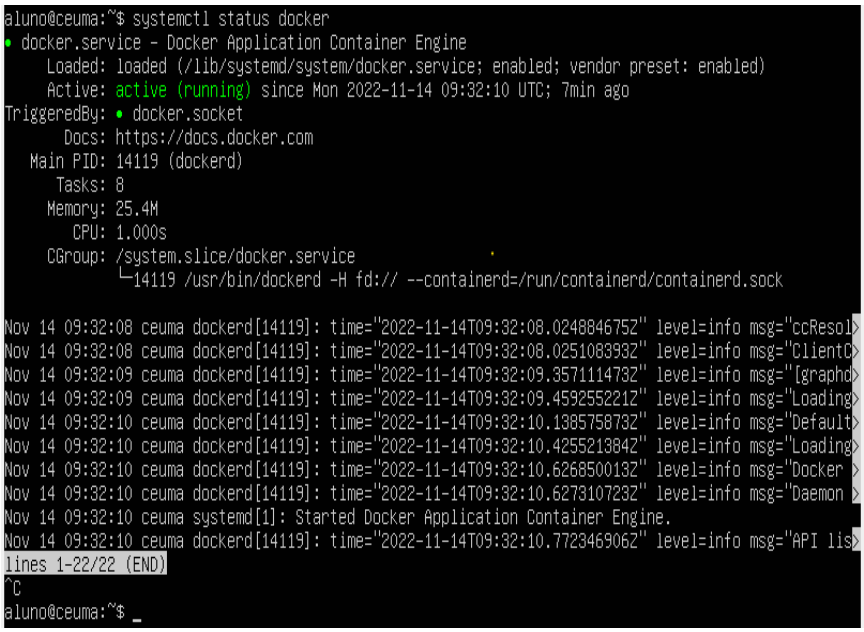
Fonte: Autoral, 2022.

O comando acima baixa uma imagem de teste e executa em um contêiner, ao ser executado, ele devolve com uma mensagem de confirmação.

O comando a seguir foi usado para verificar a atividade dos serviços do Docker:

$ systemctl status docker

Figura 3. Verificando a atividade do docker.



Fonte: Autoral, 2022.

Através desse comando, temos o controle das bibliotecas do docker e verificando sua atividade.

8.2 Criando uma chave privada

O GnuPG é uma ferramenta *open source* para comunicação e armazenamento segura de dados, que pode ser usado por linha de comando para criptografar dados e criação de assinaturas digitais.

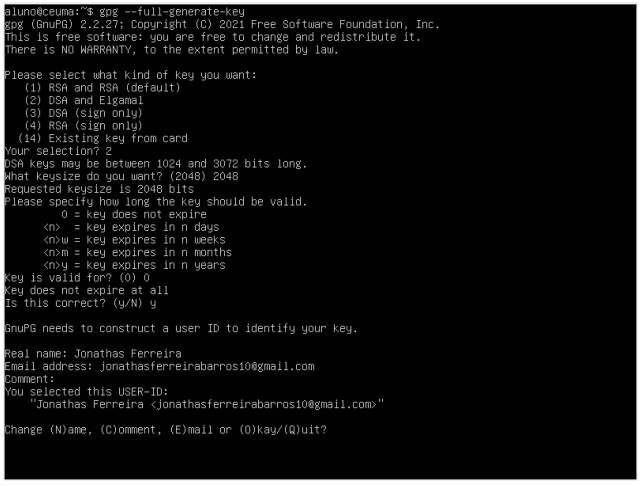
Este utiliza-se do método de criptografia conhecido como chave assimétrica,em que duas chaves são criadas: a primeira pública servindo para qualquer pessoa codifique mensagens e arquivos de modo à apenas decodificar: a segunda privada que deve ser mantida em segredo pois a mesma serve para decodificar as mensagens criptografadas.

Para que possa ser utilizado foi instalado o gnupg, com o seguinte comando:

$ sudo apt-get install gnupg

Após sua instalação é necessário construir seu diretório que armazenará suas chaves: *$ gpg* Para que as chaves sejam geradas usa-se o comando *$ gpg --full-generate-key*

Figura 4. Criação do par de chaves para assinatura.



Fonte: Autoral, 2022.

O próximo passo é escolher o tipo de criptografia que a chave vai receber e por quanto tempo a chave será válida.

Em seguida, todos os dados fornecidos serão apresentados novamente pedindo para confirmação ou edição.

Figura 5. Criação da senha.

Fonte: Autoral,2022.

A senha vai identificar a pessoa como proprietário da chave privada, pode conter espaços, não tem limite de caracter e deve obrigatoriamente conter ao menos um número.

Normalmente as pessoas assinam um arquivo para garantir ao destinatário que você é a pessoa que realmente está enviando o arquivo, para isso vamos assinar o arquivousando o comando:

$ gpg --sign jonathas.txt (nome do arquivo criado com um texto dentro)

Assinando o arquivo, em seguida será solicitado a senha que foi criada anteriormente, arquivo novo é gerado com a extensão *.gpg*.

Figura 6. Arquivo assinado e criptografado.

Fonte: Autoral, 2022.

Pode-se verificar a assinatura do arquivo usando *$ gpg --verify jonathas.txt.gpg (nome do arquivo com a extensão .gpg)*

A chave pública pode ser enviada a um servidor do keyserver ou outro servidor alternativo. A chave pública pode ser distribuída a outros usuários a fim de que possam enviar dados criptografados ou checar a autenticidade de qualquer arquivo, para isso usa- se:

$ gpg –export -a Jonathas Ferreira

Após a criação do arquivo deve-se subir o mesmo para o contêiner do docker, para tanto usaremos o comando:

$ pwd

$ls

$ mkdir docker2

$ cd docker2

Os comandos acima mostram em qual diretório nos encontramos, em seguida listamos os arquivos dentro do mesmo e criamos um diretório novo, entramos no diretório novo e criamos um arquivo *Dockerfile* dentro deste arquivo vai conter argumentos e instruções para puxar a imagem que usamos mais acima do *ubuntu*.

Para subir o arquivo para o nosso container usamos o comando:

$ sudo docker build .

O comando acima fará com que o nosso arquivo *Dockerfile* puxe a imagem, no entanto, para que possamos rodar precisamos mudar o nome do repositório com o comando:

$ sudo docker build -t ubuntu: 18.04

$ sudo docker images

Com o segundo comando conseguiremos ver o nome do repositório, seu espaço e data de criação. O comando *$ sudo docker run -it er ubuntu bin/bash* abrindo o terminal e iniciando com o container.

Para listar os containers ativos usamos o *$ sudo docker ps -a* e será listado o statuscom o tempo de criação, container e a *image*.

8.3 Solução

O questionamento feito no início deste artigo, mostra que o problema foi solucionado usando o docker, virtualização obedecendo os princípios da LGPD de proteger os dados

enviados ou recebidos e quanto a sua permissão para divulgação ou restrição desses dados, usando gnupg pode-se selecionar os arquivos que devem ser assinados com a extensão txt, a fim de criptografar e garantir a autenticidade do arquivo que chegará ao destinatário.

O docker e a virtualização fazem uma ponte como facilitador trazendo recursos que não são encontrados em todos os sistemas podendo assim garantir e trazer confiabilidade e segurança em seus recursos e na assinatura do arquivo, vistoque este é um dos pontos que a LGPD vem tratar a segurança que o usuário tem paracom o arquivo que ele está acessando vindo de uma pessoa ou demais sites da internet garantindo que o mesmo não seja um arquivo anônimo tendo um identificador para o usuário.

CONCLUSÃO

Assim como visto no decorrer do presente estudo, notou-se que a exposição de dados no âmbito virtual se caracteriza enquanto problemática coletiva, que afeta uma parcela significativa dos internautas, considerando os vários episódios de vazamento de dados, em redes domésticas e nas grandes empresas, trazendo insegurança aos usuários e ineficiência da privacidade e tutela de dados. Reconhecer os dados enquanto recurso Valioso na esfera eletrônica evidencia sua relevância e influência no ambiente digital, em várias perspectivas no dia a dia do hodierno mundo globalizado.

Os contêineres são abstrações na camada do aplicativo que empacota o código e suas dependências. Múltiplos contêineres podem ser executados em uma única máquina e compartilhar o kernel do sistema operacional com outros contêineres, cada qual executando como processos a parte no espaço do usuário. Os contêineres tomam menos espaço do queas máquinas virtuais, podendo lidar com vários aplicativos e exigindo menos da máquina virtual e sistemas operacionais (DOCKER, 2022).

O docker foi usado para virtualizar o sistema kernel do Linux Ubuntu, através de uma imagem no qual contém dados e metadados do sistema necessários para validação de chaves e até mesmo criptografia se necessário, o último não foi abordado neste presente trabalho ficando como sugestão para futuros aprimoramentos.

Desse modo, para solucionar o problema levantado no início do trabalho utilizou-se da ferramenta gnupg (GNU Privacy Guard) onde fez-se a importação de chave e assinatura do arquivo com a chave gpg. Pode-se utilizar para definir sua data de expiraçãodefinida em

dias, semanas, meses, anos em seguida a chave foi criada e importada para o arquivo assim a mesma pode ser validada e verificada.

A validação da pessoa física e jurídica é importante porque a LGPD vem tratar destes princípios para que se tenha um controle tanto por parte do controlador dos dados quanto do operador garantindo transparência em todo o seu processo observando que a lei coloca a transparência como um dos princípios principais e descosiderando o anonimato de qualquer dado.

Ao assinar é esperado que a pessoa que envia é realmente a proprietária do arquivo assim é solicitado a senha novamente, em seguida uma extensão *.gpg* então gerado o arquivo, após ser assinado pode-se checar a assinatura ou recuperar o arquivo.

Desta forma, a segurança em relação a qualquer dado dentro de qualquer arquivo texto ou pdf fica assegurada tanto pela segurança garantido pelo docker quanto pelo assinador digital. Fica o incentivo aos futuros leitores a melhorarem a segurança do projetoachando formas de tentar invadir e o autor ser avisado da violação do arquivo e seus dadosusando uma outra alternativa do docker como a exemplo o kubernetes, que possui uma documentação vasta onde um dos tópicos a serem virtualizado é o gerenciamento de segurança.

REFERÊNCIAS

Brasil. Lei 13.709 de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais ealtera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da República Federativa do Brasil, 15 agosto de 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados. Brasília, DF, agosto de 2018.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

GUEDES, Marylene. No final das contas: o que é o Docker e como ele funciona?. **TreinaWeb.** Disponível em: https://www.treinaweb.com.br/blog/no-final-das-contas-o-que-e-o-docker-e-como-ele-funciona. Acesso em: 25 outubro. 2022.

LIRA, Marcia. VirtualBox: Saiba o que é, como funciona e como instalar! **B2B Stack,** 14 setembro. 2021. Disponível em: https://blog.b2bstack.com.br/virtualbox/. Acesso em: 28 outubro. 2022.

PEREIRA, Caique Silva. **SISTEMA DISTRIBUÍDOS.** Londrina: Editora E Distribuidora Educacional S.A, 2019.

SHAMIRE, Jordan; FALCÃO, Luis. 5 Benefícios da virtualização. **IBM**, 27 abril. 2021. Disponível em: https://www.ibm.com/blogs/digital-transformation/br-pt/5-beneficios-da-virtualizacao/. Acesso em: 28 outubro. 2022.

SILVEIRA, Sergio Amadeu da. **Tudo sobre todos: Redes digitais, privacidade e vendade dados pessoais.** São Paulo: Edições Sesc, 2017.

Use contêineres para construir, compartilhar e executar seus aplicativos. **Docker**. Disponível em: https://www.docker.com/resources/what-container/. Acesso em: 25 outubro. 2022.