MONITORAMENTO DE BACKUP: conferência de erros durante a realização do backup local

AMANCIO, Rafael[1]; TREVIZANO, Waldir A.[2]; PEREIRA, Ana Amélia de Souza[3]; DAIBERT, Marcelo Santos[4]

[1] Graduação em Ciência da Computação - UNIFAGOC
[2] Docente do curso de Ciência da Computação - UNIFAGOC
[3] Docente do curso de Ciência da Computação - UNIFAGOC
[4] Docente do curso de Ciência da Computação - UNIFAGOC

rafaeldasilva1110@gmail.com
waldir@unifagoc.edu.br
ana.amelia@unifagoc.edu.br
daibert@unifagoc.edu.br

RESUMO

Os dados gerados em uma empresa são de extrema importância, portanto a realização de cópias de segurança (backups) ganha destaque. Além da ação em si, o monitoramento deve garantir que esses processos sejam executados da forma correta. Este projeto teve como objetivo a implementação de uma ferramenta para o monitoramento de backup. Foi desenvolvida uma dashboard, em ambiente desktop, com responsividade para navegadores de dispositivos móveis, utilizando linguagens de programação como PHP, CSS, HTML e banco de dados MySQL. O monitoramento com a nova ferramenta resultou em ganho de performance, demonstrando o quanto a empresa em que foi implementado esse serviço ganha no desempenho dos analistas em conjunto com uma precisão de informações sobre os backups.

Palavras-chave: Backup. Monitoramento. Scripts. Segurança da informação. Banco de dados.

INTRODUÇÃO

À medida que as empresas se desenvolvem, seus dados e informações se tornam cada vez mais cruciais para seu desenvolvimento e lucratividade. Uma forma eficaz de guardar esses dados, é a utilização de sistemas de gerenciamento de bancos de dados. Algumas empresas, para armazenar dados, usam diversos sistemas gerenciadores; contudo, mesmo que todos os gerenciadores trabalhem de formas parecidas, a diferença entre eles é somente o seu desempenho durante o uso. Esses dados, independentemente de como são armazenados, devem ser mantidos de uma forma confiável, porque isso é importante para o crescimento organizacional de uma empresa.

Bancos de dados são estruturas nas quais os dados são armazenados, podendo ser em uma máquina local, em um servidor na empresa dedicado para isso ou então num serviço online (nuvem), em que o usuário possa acessá-los a qualquer momento.

A segurança da informação é uma preocupação importante, principalmente após a criação da LGPD (Lei Geral de Proteção de Dados). A LGPD tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção dos dados

A intenção é manter os dados protegidos contra danos, perdas, falsificação e garantir a confidencialidade necessária para evitar a interrupção dos negócios e mitigar os riscos. nesse aspecto, Netto e Silveira (2007, p. 1) ensinam: "As ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados". Isso corrobora que se está exposto ao mesmo tipo de ameaça em ambos os mundos, seja no mundo virtual, seja no mundo físico.

Assim, para se precaver contra a perda dos dados, é necessário realizar uma cópia de segurança ou *backup* dos arquivos gerados pelo banco de dados. O *backup* tem como propósito criar uma cópia exata dos arquivos, armazenando-os em outro local. Essa cópia poderá ser usada em casos como uma perda de dados, destruição, alterações incorretas, corrupção ou um ataque de vírus, que na maioria das vezes causam um sequestro dos dados e/ou criptografia dos dados.

O monitoramento desse tipo de processo, o monitoramento de *backup*, precisa ser feito de forma minuciosa e dinâmica, principalmente quando existem diversos sistemas diferentes, com diversos clientes. Em empresas com vários sistemas em operação, uma tarefa vital é monitorar se os diversos backups desses sistemas estão sendo feitos de forma correta. Na cidade de Ubá-MG, em uma empresa que presta serviço de backup, existe um monitoramento desses dados via e-mail, sendo enviadas algumas informações importantes do backup, porém, o aumento do número de seus clientes implicou um envio massivo diário de e-mails, dificultando a visualização dos erros ocorridos devido à quantidade a ser consultada. Com isso, foi identificada a necessidade de melhorar a efetividade do monitoramento, a fim de facilitar a identificação e a leitura de um possível erro que possa ter acontecido.

Portanto, o objetivo deste projeto é realizar um monitoramento dos arquivos de backup que são separados diariamente nos processos de extração, compactação e *Yesterday (*termo em inglês usado para referenciar os arquivos do dia imediatamente anterior), usado nos casos em que a empresa precise de uma recuperação mais recente dos arquivos, pretendendo desse modo melhorar a eficiência e a qualidade da resolução de problemas relacionados ao *backup* dos clientes.

São os seguintes os objetivos específicos da aplicação:

- Melhorar a visualização da informação relacionada aos backups feitos em uma dashboard;
- Filtrar com mais assertividade erro que esteja acontecendo no processo de backup do cliente;
- Diminuir o volume de e-mails recebidos dentro da empresa referente a problemas na execução;
- Visibilidade dos resultados de backup em mais plataformas além da máquina onde o responsável pela análise trabalha.

REFERENCIAL TEÓRICO

Tipos de Backups

Tipos de backups são uma parte importante do planejamento de proteção de dados e continuidade dos negócios. Os tipos mais comuns de backups são o completo, o incremental e o diferencial. O backup completo copia todos os dados do sistema, enquanto o backup incremental copia apenas os dados que foram modificados desde

o último backup completo; já o backup diferencial copia apenas os dados que foram modificados desde o último backup completo ou incremental (Kiboi, 2017).

A escolha do tipo ideal de backup depende de vários fatores, incluindo a frequência de mudanças nos dados, o tempo disponível para backups e a capacidade de armazenamento de backups (Kiboi, 2017). Em um estudo realizado por Kiboi (2017), verificou-se que o backup incremental é a opção mais viável em ambientes com alta frequência de mudanças nos dados, enquanto o backup completo é a melhor escolha em ambientes com baixa frequência de mudanças.

Além disso, é importante considerar a segurança dos dados ao escolher o tipo de backup adequado. De acordo com um estudo realizado por Smith (2019), o armazenamento em nuvem é uma opção segura e acessível para backups, mas é importante considerar as políticas de segurança da nuvem antes de optar por essa opção.

Armazenamento de Backups

Armazenamento de backups é uma parte crucial da estratégia de proteção de dados, pois garante a disponibilidade dos dados em caso de falha no sistema principal. Existem várias opções de armazenamento de backups, incluindo discos rígidos externos, unidades de fita, armazenamento em nuvem e outros (Wang, 2018). A escolha do armazenamento adequado depende de vários fatores, incluindo a quantidade de dados a serem armazenados, a necessidade de acessibilidade e a segurança dos dados (Wang, 2018).

De acordo com um estudo realizado por Johnson (2019), o armazenamento em nuvem é uma das opções mais populares para armazenamento de backups, devido à sua escalabilidade, disponibilidade e flexibilidade. Além disso, segundo o autor, o armazenamento em nuvem também permite a recuperação de dados em caso de falha no sistema principal, sem a necessidade de hardware físico.

Outra opção de armazenamento de backups é o uso de discos rígidos externos. Esse tipo de armazenamento é fácil de usar e oferece baixo custo, mas pode não ser a melhor escolha em termos de segurança dos dados (Wang, 2018).

Em conclusão, a escolha do armazenamento adequado para backups é crucial para garantir a disponibilidade e a segurança dos dados. A opção de armazenamento ideal depende de vários fatores, incluindo a quantidade de dados a serem armazenados, a necessidade de acessibilidade e a segurança dos dados (Wang, 2018).

Teste e Validação de Backups

Teste e validação de backups é uma parte importante da estratégia de proteção de dados, pois garante que os dados possam ser recuperados de forma eficiente em caso de falha no sistema principal. A validação dos backups inclui a verificação da integridade dos dados e a confirmação de que eles possam ser recuperados corretamente (Smith, 2016).

De acordo com um estudo realizado por Brown (2017), a realização de testes regulares de recuperação de dados é essencial para garantir que os backups estejam funcionando corretamente. Além disso, o estudo também destaca a importância de testar os backups em um ambiente diferente do sistema principal, pois isso garante que eles possam ser recuperados corretamente em caso de falha no sistema principal (Brown, 2017).

Outra abordagem para teste e validação de backups é o uso de softwares de simulação de falhas, que permitem testar a recuperação de dados em caso de falhas previstas ou não previstas (Smith, 2016). Esses softwares também podem ser usados para testar a eficiência dos processos de recuperação de dados, incluindo o tempo de recuperação e a integridade dos dados recuperados (Smith, 2016).

Em conclusão, teste e validação de backups é uma parte importante da estratégia de proteção de dados. A realização de testes regulares de recuperação de dados e o uso de softwares de simulação de falhas garantem que os dados possam ser recuperados de forma eficiente em caso de falha no sistema principal (Smith, 2016; Brown, 2017).

MATERIAIS E MÉTODOS

Para a realização do projeto, foi identificado que a dificuldade de monitorar os backups realizados se deveu ao volume de e-mails que estavam sendo recebidos por dia, contendo as informações de cada rotina de *backup*; com isso, as análises demoravam, gerando atraso na visualização dos erros e consequentemente uma correção mais lenta desses erros no backup.

O ambiente de trabalho usado para realizar a implementação do painel Web de monitoramento de *backup* foi o Windows, devido à facilidade de visualização e instalação de ferramentas que possam auxiliar no desenvolvimento. Além disso, foi levada em consideração a utilização diária do sistema operacional, que também ajuda na construção da aplicação. Foi usada a IDE Visual Studio Code para realizar a criação e testes dos códigos-fonte criados, já que permite que se possa trabalhar com diversas linguagens de programação simultaneamente, garantindo agilidade na escrita dos códigos e facilitando os testes que devem ser realizados;

Para que possa ser feito o envio do relatório de cada uma das etapas do backup local de cada um dos clientes, foi criada uma API (Application Programming Interface), para que cada etapa possa se comunicar com o servidor e fazer o envio do relatório. O Código 1, a seguir, apresenta como foi desenvolvido o script de monitoramento para se usar no ambiente Windows.

Código 1 - API

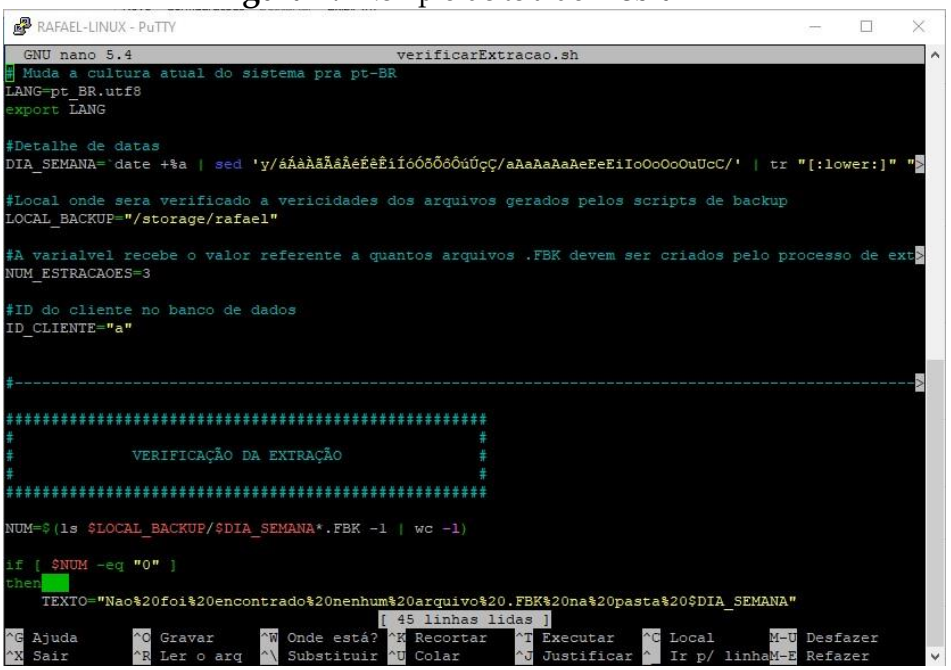
```
include("conexao.php");
header("Access-Control-Allow-Origin: *");
$recid=$_GET["id"];
$status= $_GET["status"]; $msg =
$_GET["msg"];
$Object = new DateTime();
$Object->setTimezone(new DateTimeZone('America/Sao_Paulo'));
$DateAndTime = $Object->format("Y-m-d H:i:s");
$sql = "UPDATE cliente_backup SET hd = '$status', msghd = '$msg',
last_alert_hd = '$DateAndTime' WHERE idEmpresa = '$recid'"; mysqli_query($conexao, $sql);
```

Fonte: dados da pesquisa.

Já para realizar a criação dos scripts de monitoramento para o ambiente Linux, foi usada a distribuição Debian 11, que foi escolhida por ser um sistema leve, com fácil configuração para a utilização diária do sistema. O sistema é configurado sem a utilização de interfaces para melhorar a sua segurança com os dados empresariais e o

seu desempenho durante o uso. A Figura 1 mostra a forma de visualização do sistema operacional Debian 11.

Figura 1: Exemplo de tela do Debian 11



Fonte: dados da pesquisa.

Durante o desenvolvimento, a empresa queria uma forma mais simples de se visualizar os erros. Para isso, foi apresentado o formato em *dashboard,* onde seriam exibidas somente informações relevantes para a conferência do *backup.* Na sua implementação, foram usados o HTML (HyperText Markup Language), o CSS (Cascading Style Sheets) e as linguagens de programação JS (JavaScript) e PHP (Personal Home Page).

As linguagens HTML e CSS foram usadas para fazer a parte visual da dashboard. Com elas, foi possível fazer tabelas e pop-ups para melhorar a visibilidade de um erro encontrado durante o relatório de monitoramento. Trabalhando juntamente a elas, foi usado o JavaScript, para que se pudesse fazer as modificações na parte visual, de acordo com o relatório de backup. Foram escolhidas as cores: verde, para uma confirmação que o backup está funcionando corretamente; e vermelho, para um problema relacionado ao processo de backup. A seguir, a Figura 2 mostra uma pequena parte do código-fonte desenvolvido para a página de login; e na Figura 3 visualiza-se o resultado obtido (Figura 3).

Figura 2: Código-fonte

```
<article>
    <div class="containerLogin">
        <div class="boxLogin">
            <span class="titlelogin">Backup - Certa Soluções</span>
            <div class="login">
                <div>
                    <form action="" method="POST">
                        <p>
                            <input type="text" name="usuario" placeholder="Nome de usuario" />
                        </p>
                        <p>
                            <input type="password" name="senha" placeholder="Senha" />
                        </p>
                        <p>
                            <button type="submit" class="bntLogin">Login</button>
                        </p>
                    </div>
                </div>
            </div>
    </div>
</article>
```

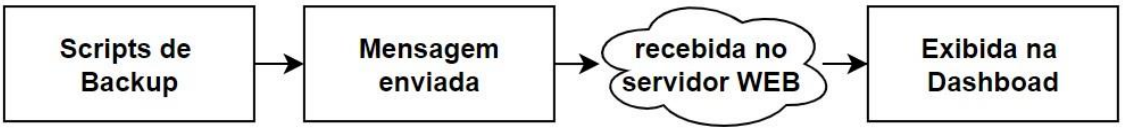
Fonte: dados da pesquisa.

Figura 3: Resultado do código-fonte

Fonte: dados da pesquisa.

Com tudo configurado, e usando as informações do servidor do cliente e as informações de cadastro na plataforma *Web*, o fluxo de informação do servidor do cliente até a sua visualização deve estar de acordo com o fluxograma apresentado na Figura 4.

Figura 4: Fluxo de relatório

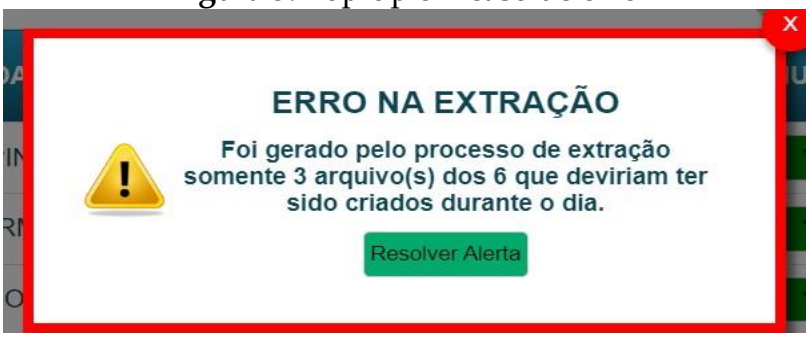


Fonte: dados da pesquisa.

A dashboard se comunica com o banco de dados em que as mensagens de erro, ou de sucesso, são armazenadas; em seguida, são exibidas para o usuário de forma otimizada. Clicando em alguma das mensagens que está apresentando erro,

apresentadas na colocação vermelha, será exibido um pop-up (Figura 5), em que serão mostrados detalhes do erro ocorrido; com isso, já será analisada a correção do problema, para não prejudicar o funcionamento da rotina.

Figura 5: Pop-up em caso de erro



Fonte: dados da pesquisa.

Caso o problema seja resolvido, em uma conexão ao servidor do cliente, por exemplo, não é preciso aguardar até o outro dia para uma próxima verificação: pode-se ter a ação de colocar o alerta como resolvido, clicando no botão que irá aparecer no pop-up.

RESULTADOS E DISCUSSÃO

Scripts dos Sistemas

Na implementação do sistema, para avaliar qual seria a melhor forma de fazer a coleta dos dados de *backup* de cada um dos clientes, ficou-se entre a criação de uma aplicação que ficaria em segundo plano a todo momento realizando a coleta e as tarefas automatizadas do próprio sistema, os *scripts*. Foram escolhidos os scripts, devido a uma implementação mais ágil das tarefas e por trabalharem diretamente com o sistema operacional. É uma forma de executar somente em determinados momentos com o auxílio dos gerenciadores de tempo do sistema, pois uma aplicação criada teria que ser mantida em segundo plano para que pudesse fazer a coleta dos dados. e isso poderia, em algumas ocasiões, causar lentidão e até mesmo incompatibilidade em algum sistema operacional, seja por versão ou mudança de ambiente.

Com a opção dos scripts *Power Shell* e *Shell Script* para fazer a coleta, primeiramente foi criada uma API (Application Programming Interface) para que se comunicasse com o banco de dados de uma forma mais segura.

Dashboard

Foi implementada uma *dashboard* como forma de visualizar o relatório de backup dos clientes. sendo possível visualizar diversas informações simultaneamente, além de permitir identificar em qual processo do backup, se extração, compactação ou *Yesterday*. Esse termo – "ontem", em inglês – é usado na empresa se houver necessidade de fazer uma recuperação mais recente do arquivos ou caso um problema tenha feito com que o backup não finalizasse da forma adequada.

Uma visualização da *dashboard* da ferramenta está apresentada na Figura 6, em que são exibidas algumas informações importantes do relatório que foi enviado via API para o banco de dados. A separação das diversas informações é feita por uma tabela, em que cada linha significa um cliente no qual esteja configurado o

monitoramento de backup. Nessa linha apresenta-se o sistema operacional, o nome do cliente e o status de cada uma das etapas do backup.

Figura 6 - *Dashboard*

Fonte: dados da pesquisa.

Para visualizar com mais detalhes o erro que possa ter ocorrido em um dos clientes, basta clicar no botão correspondente ao erro (os que estão em vermelho), que será exibido um *pop-up* (conforme apresentado na Figura 5), com uma pequena descrição do erro que possa auxiliar na sua resolução.

Foram utilizadas duas cores para as notificações: verde e vermelha. Segundo Pedrassolli e Néris (2014), a segunda estimula o entusiasmo, dinamismo, ação ou violência, dando uma sensação de calor e força; já a primeira transmite uma sensação de equilíbrio, bem-estar e tranquilidade, funciona como um sedativo que tem efeito de reduzir a pressão sanguínea. O emprego dessas cores nos status de erro e de sucesso possibilita, além da informação do status do *backup*, uma análise mais rápida.

Uma vez que os dispositivos móveis, como tablets e smartphones, estão sendo cada vez mais utilizados, manter uma boa visibilidade de informação neles tem um resultado ainda mais satisfatório para uma consulta rápida de um status e até mesmo para mostrar a ferramenta para um cliente que já tem o serviço, além de conseguir estender para uma outra pessoa que possivelmente possa estar precisando desse tipo de serviço. Na Figura 7, a seguir, visualiza-se a mesma tela vista anteriormente na Figura 6, porém em um navegador de um celular.

Figura 7 - Visualização em dispositivo móvel

Fonte: dados da pesquisa.

Como a ferramenta foi desenvolvida para navegadores web, o acessar em um dispositivo móvel, celular ou smartphone, possibilita obter as mesmas informações que teríamos em um computador ou notebook.

Após a implementação da ferramenta, foi observado que, além de ganho no tempo de resposta para um erro que acontecia em um dos processos, houve também uma diminuição na quantidade de erros recebidos pelo e-mail sem correção: o que antes chegava por volta de 70 e-mails diário passou a ser uma média de 10-20, podendo esse valor ainda ser diminuído, à medida que o tempo for passando e as correções fiquem ainda mais assertivas, para não apresentar mais falhas.

CONCLUSÃO

Mediante os resultados obtidos após o desenvolvimento e implementação da ferramenta em todos os clientes, o monitoramento e a análise do tempo gasto para conferência de um *backup*, é cabível afirmar que o ganho de tempo e o desempenho no monitoramento dos *backups* foram satisfatórios, já que, na *dashboard,* as informações já vêm filtradas para o usuário, e, com a utilização de recursos visuais para a percepção de resultados, podem ainda ser mais rápidas e precisas em cada análise.

Com essa ferramenta, a empresa pode automatizar o monitoramento de *backup,* possibilitando que o analista faça outras tarefas com o tempo que foi reduzido no monitoramento de *backups,* permitindo que a empresa consiga analisar outros pontos que possam ser melhorados e automatizados com a ferramenta apresentada.

No sistema desenvolvido, ainda podem ser feitas diversas melhorias no sistema, por exemplo, não depender do sistema operacional para auxiliar na execução dos scripts de verificação e, além disso, melhorar as interfaces gráficas da aplicação e o desempenho, destacando ainda mais o projeto.

REFERÊNCIAS

ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. **Informação e Sociedade: Estudos**, v. 20, n. 1, p. 155-168, 2010.

CERT.br. Ransomware: saiba como se prevenir desse código malicioso com as orientações do CERT.br. Disponível em: https://www.tiespecialistas.com.br/review/ransomware-saiba-como-se-prevenir-desse-codig o-malicioso-com-as-orientacoes-do-cert-br/. Acesso em: 21 set. 2022.

DIOGENES, Yuri; MAUSER, Daniel. **Certificação Security +**. Novaterra, 2011.

FEW, S. **Information dashboard design:** the effective visual communication of data. Itália: O'Reilly, 2006. 223 p.

JESUS, Guilherme Bindi Alencar; SCHMIGUEL, Juliano. Implementação de Backup como processo de segurança da informação. **Revista Atlante: Cuadernos de Educación y Desarrollo,** fev. 2018. Disponível em: https://www.eumed.net/rev/atlante/2018/02/backup-seguranca-informacao.html. Acesso em: 22 set. 2022.

JOHNSON, J. Cloud storage as a backup solution. **Journal of Cloud Computing**, v. 8, n. 4, p. 65-70, 2019.

KIBOI, J. Types of backups and their use in data protection. **Journal of Data Protection and Recovery**, v. 5, n. 2, p. 23-28, 2017.

MACHADO, Rômulo Galvão; PILAN, José Rafael. Estudo e desenvolvimento de uma ferramenta de workflow para o monitoramento de backup-dashbackup. **Tekhne e Logos**, 2020, v. 11, n. 1, p. 50-59.

MEDRADO, Heitor. **BACULA:** ferramenta livre de backup. Rio de Janeiro: Brasport, 2010.

PEDRASSOLLI, L. C.; NÉRIS, V. P. A. O uso de cores em aplicações web: um estudo dos projetos desenvolvidos no curso lato sensu de desenvolvimento de software para a web. **Revista TIS**, São Carlos-SP, v. 3, n. 2, p. 204-214, 2014.

PIMENTA, A. M. S.; QUARESMA, R. F. C. A segurança dos sistemas de informação e o comportamento dos usuários. **JistemJ.Inf.Syst. Technol. Manag**, São Paulo, v. 13, n. 3, p. 533-552, 2016. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S180717752016000300533&lng=en &nrm= iso. Acesso em: set. 2022.

SMITH, J. Cloud storage for backups: benefits and risks. **Journal of Cloud Computing**, v. 8, n. 4, p. 56-62, 2019.

WANG, L. Options for backup storage**. Journal of Data Protection and Recovery**, v. 6, n. 1, p. 35-40, 2018.