https://doi.org/10.22491/2357-9730.105781

Segurança e legitimidade no trabalho remoto: relato de experiência em um hospital público e universitário

Security and legitimacy in remote work: an experience report in a public teaching hospital

Milena de Avila Peres[1], Gabriel Alabarse Hernandez[1], Daniel da Silva Jegorschki Santos[1], Silvia Regina Gralha[1], Renato Falsarella Martins Malvezzi[1]

RESUMO

Este relato de experiência tem como objetivo apresentar os esforços necessários em uma das ações de enfrentamento à COVID-19 no Hospital de Clínicas de Porto Alegre: viabilizar teletrabalho. Na iminência de criar uma estrutura tecnológica de preservação da operacionalidade da força de trabalho, foi necessário adotar medidas que permitissem a atuação remota dos colaboradores em atividades administrativas de apoio à assistência. Com este desafio desenvolveu-se, em curto espaço de tempo, uma solução técnica segura que permitisse acesso externo aos sistemas corporativos e registro eletrônico de frequência em regime de trabalho remoto. Além de ferramentas de apoio como: plataforma em nuvem para reuniões não presenciais, para documentos eletrônicos, etc. Desta forma, foi possível disponibilizar aos colaboradores do hospital, que não atuam na linha de frente, a atuação remota de seu trabalho.

Palavras-chave: *Trabalho remoto; teletrabalho; home office; registro de frequência; acesso externo; Covid-19*

ABSTRACT

This experience report aims to present the necessary efforts in one of the actions to confront COVID-19 at Hospital de Clínicas de Porto Alegre: enabling teleworking. In order to create a technological structure that would preserve the workforce's operability, measures were adopted to allow remote performance of employees in administrative support activities. With this challenge, a secure technical solution was developed in a short period of time, allowing external access to corporate systems and electronic frequency records in a remote work regime. Also developed were support tools such as a cloud platform for non-face-to-face meetings, for electronic documents, etc. Thus, remote performance of activities was made available to hospital employees who do not work at the front line.

Keywords: *Remote work; teleworking; working from home; frequency record; external access; Covid-19*

Clin Biomed Res. 2020;40(2):71-75

1 Hospital de Clínicas de Porto Alegre. Porto Alegre, Rio Grande do Sul, Brasil.

Autor correspondente:
Milena de Avila Peres
maperes@hcpa.edu.br
Hospital de Clínicas de Porto Alegre
Avenida Protásio Alves, 211
90035-903, Porto Alegre, RS, Brasil

INTRODUÇÃO

No início do ano de 2020, devido a pandemia do Coronavírus, onde o distanciamento social passa a ser a palavra de ordem, empresas que não estavam preparadas para aderir ao modo de trabalho remoto, precisaram se adaptar rapidamente a fim de sustentar aos apelos e as novas rotinas de trabalho do país. Em março, a equipe de Tecnologia da Informação do Hospital de Clínicas de Porto Alegre (HCPA), iniciou as ações de disponibilização de

ferramentas para teletrabalho de forma segura e legítima até então inexistentes. A partir da publicação da Medida Provisória 927/2020[1], todos os setores e colaboradores do hospital que pudessem executar as suas funções de forma remota deveriam assim fazê-lo.

O HCPA por ser um hospital e uma empresa pública tem como compromisso de sua administração uma série de prerrogativas legais que foram estudadas por um grupo de trabalho estabelecido pela direção executiva para gestão da crise e enfrentamento à COVID-19. Como requisito desta avaliação foi colocada a necessidade de fornecer aos colaboradores acesso ao sistema de controle de frequência, fornecendo ao empregado e empregador um meio de controle legítimo da jornada de trabalho, de acordo com as as portarias 373[2] e 1510[3] do Ministério do Trabalho. Outro ponto destacado foi a necessidade de garantir que os colaboradores, ao realizarem acesso remoto nos sistemas corporativos do HCPA, utilizassem uma conexão segura, com múltiplos fatores de autenticação, conforme prevê a norma complementar 07/IN01/DSIC/GSIPR[4], de 2010, do Departamento de Segurança da Informação e Comunicações, que estabelece diretrizes de controles de acesso nos órgãos e entidades da Administração Pública Federal.

Enquanto as demais áreas do HCPA já se organizavam para o trabalho remoto, a equipe de TI precisou elaborar e implementar, em um curto espaço de tempo, uma série de mecanismos para que tal prática pudesse ser realizada.

Diante deste cenário, o objetivo deste artigo é apresentar como a equipe de TI do HCPA se mobilizou na implementação e implantação dos artefatos para que fosse possível a realização do teletrabalho, tendo como desafio estar em conformidade com a legislação trabalhista e a segurança na preservação dos dados e informações confidenciais do sistema hospitalar.

MATERIAIS E MÉTODOS

Neste artigo, usou-se a metodologia científica de natureza aplicada, com abordagem qualitativa do tipo exploratória, com métodos adequados, utilizando técnicas de observação participante.

Primeiramente foi analisado o que poderia ser feito com o que já existia, a fim de agilizarmos o processo para dar uma resposta rápida. Foi feita uma avaliação das funcionalidades já existentes no sistema de controle de frequência utilizado pelo HCPA, da qual se tomou conhecimento da existência do módulo de registro remoto, porém o mesmo não pode ser utilizado por não estar incluído nos serviços contratados atualmente pelo hospital. Foi levantada então a possibilidade de se elaborar uma solução de controle de frequência para que os colaboradores, em regime celetista, pudessem registrar seus pontos remotamente. Na sequência foram identificados desafios, onde os aspectos observados ressaltaram o tempo hábil para providenciar as liberações e questionamentos sobre quais as melhores ferramentas de TI utilizadas e recursos disponíveis no momento.

Processo de liberação ao acesso remoto com autenticação de dois fatores

Para atender a necessidade de cada usuário ter o seu acesso liberado à rede virtual privada (VPN) do HCPA foi implementado um sistema de autenticação utilizando a ferramenta *Google Authenticator*, que gera códigos de acesso únicos para cada usuário a partir da importação de um código de barras no formato *QRCode* em um aplicativo de celular. A arquitetura técnica da solução[5] se deu conforme Figura 1 abaixo:

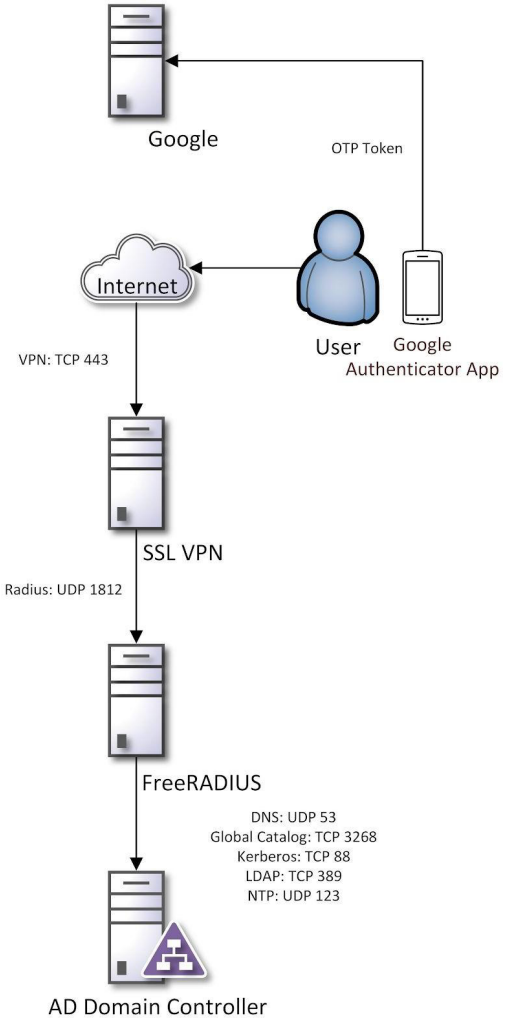

Figura 1: Arquitetura da solução de acesso remoto com dois fatores de autenticação.

Fonte: Harmonson, Richard . 2017. Two Factor Authentication using FreeRADIUS with SSSD (FreeIPA or Active Directory) and Google Authenticator on CentOS 7.

A liberação de acesso para os usuários na VPN se constituiu então de três etapas operacionais: Inclusão do usuário em grupo de acesso; Geração e envio do código *QRCode* para *Google Authenticator*; e Liberação do usuário no *firewall* do HCPA. Para evitar que a operação de liberação dos usuários fosse demasiadamente prolongada, os passos necessários para esta ação foram automatizados através de *scripts* programados e incluídos na rotina de liberação de acesso descrita abaixo.

Controle de liberação de acesso

Fazia-se necessário um mecanismo para cadastrar os usuários que teriam acesso a esta liberação, pois era requisito das áreas gerenciais que a liberação pudesse ser controlada.

Para que fosse possível a liberação do registro de frequência remoto, o colaborador precisa antes, estar ciente e concordar com os termos propostos para essa nova modalidade de trabalho. Para isso, no portal do colaborador, antes de ser disponibilizado o registro de ponto, ele preenche um formulário com suas atividades a serem realizadas, o período de disponibilização do acesso remoto, toma ciência dos termos e realiza o armazenamento das informações. Este preenchimento é encaminhado ao setor de gestão de pessoas, as chefias imediatas e coordenador.

Associada a esse preenchimento do formulário se fazia necessária uma rotina de liberação de acesso, que serviu, também, como amarração dos processos por meio de uma situação que permite o controle da liberação. Com a inclusão do formulário, o usuário recebe o estado 'NOVO', após a execução da rotina e geração do *QRCode* para o acesso à VPN, o estado é alterado para 'LIBERADO', assim também liberando à nova funcionalidade de registro de frequência para o usuário.

Registro de ponto (Controle de Frequência)

Por fim optou-se por construir uma solução proprietária e integrada, bem como o mecanismo de integração desta com o atual sistema de registro de frequência, diminuindo os impactos no restante dos processos que fazem uso da informação de registro de ponto. Funcionalidade esta que também tem controle de liberação sob demanda.

Abaixo estão listados os passos construídos para o registro do ponto remoto:

- O colaborador deve se autenticar no portal e acessar a aba **"Ponto Remoto"**;
- Tela de registro de ponto só será apresentada se colaborador tiver preenchido o formulário de solicitação descrito no item 2.2;
- Ao registrar o ponto, os dados são armazenados em uma tabela no banco de dados com auditoria. Diariamente é realizado um processo para exportar esses registros para o sistema de controle de frequência principal.

RESULTADOS

Como resultado dos estudos e pesquisas desenvolvidos foi construída a solução de forma a atender todas necessidades, de forma rápida, baixo custo e eficaz. Primeiramente foram realizados aprimoramentos na infraestrutura de TI para o acesso à rede e sistemas corporativos do HCPA. Nessa etapa, foi necessário realizar configurações para liberação de acesso no firewall bem como organizar e melhorar o processo de acesso por VPN, agregando um segundo fator de autenticação de forma a manter o mais alto padrão de segurança para proteger os sistemas e dados corporativos de ataques maldosos externos. Visto se tratar de algo novo para a maioria dos colaboradores, foram desenvolvidos manuais, e posteriormente pequenos vídeos, a fim de auxiliar que cada um conseguisse configurar seu próprio ambiente de trabalho remoto e ter acesso aos sistemas do Hospital.

Em segundo lugar se desenvolveu o módulo do 'Ponto Remoto' dentro do Portal do Colaborador na intranet do Hospital. Este viabilizou, de forma integrada, a solução para disponibilização o *QRCode* do colaborador, utilizado na configuração do mecanismo de autenticação conforme descrito no item 2.1, o preenchimento do formulário de solicitação de liberação de acesso relatado no item 2.2 e o registro do ponto propriamente dito de acordo item 2.3.

Na Figura 2 consta a tela para os colaboradores que ainda não obtiveram o acesso remoto e precisam de orientações para fazê-lo. Contém também os links do formulário de liberação e do '*Hotsite*' de manuais, e tutoriais em vídeo.

Na Figura 3 um acesso de usuário que já possui a liberação, desta forma fica disponível o *QRCode* para instalação do mecanismo de autenticação em duas etapas/fatores bem como a opção do registro do ponto, o histórico e acesso ao acordo previamente preenchido.

Por fim a etapa de integração dos registros que são realizados no referido módulo, mediante autorização e autenticação prévias de cada colaborador, armazenados em banco de dados seguro e com auditoria, com o sistema principal de registro de frequência do HCPA.

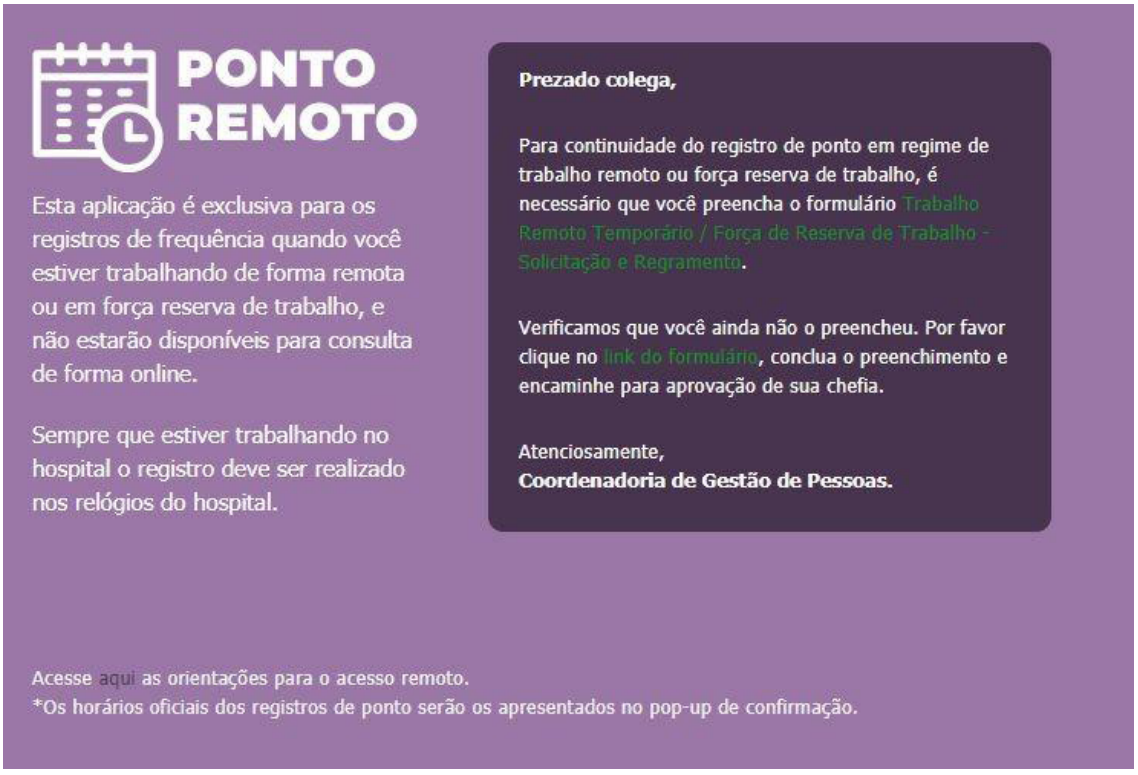

Figura 2: Interface ponto remoto/solicitação de acesso.
Fonte: Hospital de Clínicas de Porto Alegre.

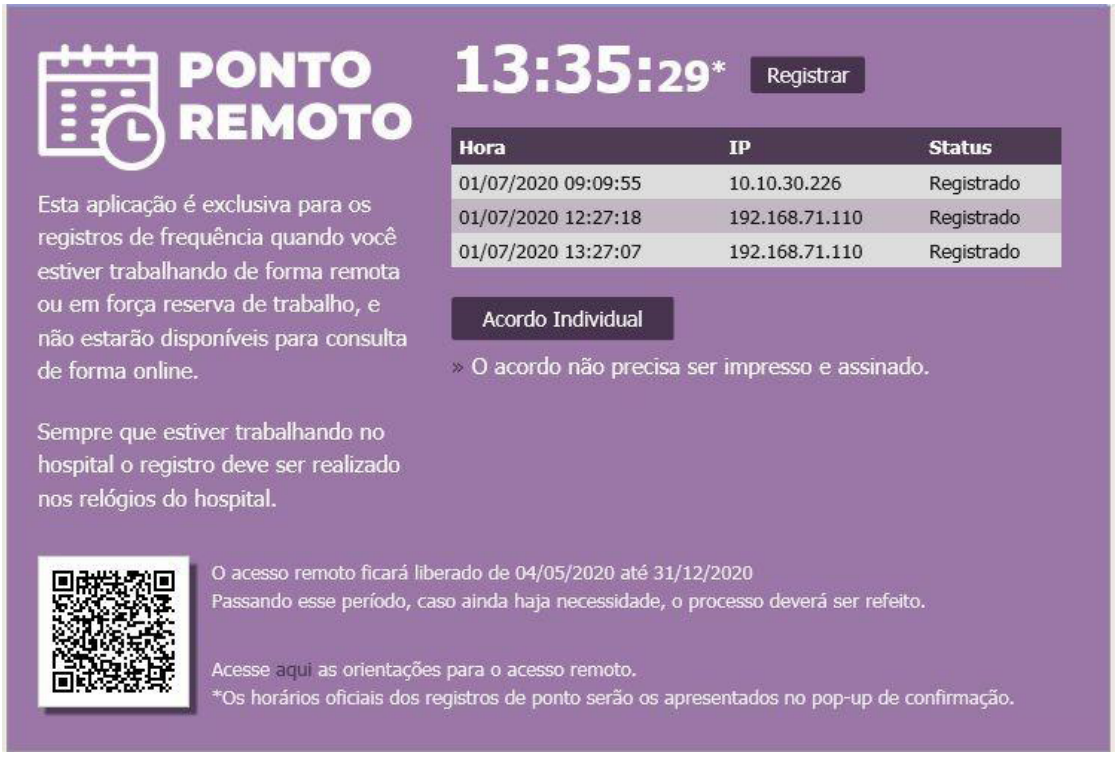

Figura 3: Interface ponto remoto/registro do ponto.
Fonte: Hospital de Clínicas de Porto Alegre.

Tal serviço consiste em um *script* que está agendado para executar automaticamente e que realiza o acesso a esse banco de dados lendo os registros efetuados, dia a dia, e criando um arquivo para troca de dados que é salvo diretamente para o servidor onde é importado pelo sistema principal de controle de frequência.

A solução concebida foi desenvolvida em poucos dias, montado o ambiente e disponibilizado aos colaboradores essa nova modalidade de trabalho. A partir daí, além do acesso aos sistemas corporativos para execução das atividades de rotina, as reuniões de trabalho passaram a ser virtuais. É utilizada principalmente a ferramenta "Google Meeting", um serviço de comunicação por vídeo desenvolvido pelo Google e o "Google Hangout", que permite troca de mensagens rápidas – *'chats'* entre os colaboradores. Com a solução em operação, as chefias de cada setor do hospital passaram a avaliar e direcionar seus colaboradores para a nova modalidade de trabalho.

DISCUSSÃO

Após todos os desafios vencidos pela equipe de TI comprometida com o propósito do HCPA, qualquer colaborador tanto da área assistencial quanto administrativa, pode optar por trabalhar remotamente, diminuindo, assim, as chances de contaminação por Covid-19. Desta maneira, os colaboradores diminuíram os acessos nas dependências do hospital, em respeito ao distanciamento social em virtude das normas governamentais e por se tratar de um local de trabalho com alta probabilidade de contágio.

A criação de vídeos com tutoriais contendo passo a passo, bem como a disponibilização de um hotsite para colaboradores do HCPA minimizaram várias dificuldades enfrentadas durante a implantação deste novo processo de trabalho, facilitando também difundir os novos conhecimentos para mais de 7 mil usuários em poucos dias.

A velocidade de resposta e a organização interna da TI, frente a este cenário adverso, reitera o HCPA como referência na construção de soluções tecnológicas que apoiam a assistência e a gestão de saúde pública da sociedade gaúcha.

Como sugestão para trabalhos futuros, estudar os outros benefícios e impactos, como econômicos, ativos que deixaram de ser consumidos, como luz, água, papel, impressões, refeições e até mesmo a possível diminuição de acidentes de trabalho, afastamentos de saúde e horas extras com esse distanciamento e tempo no trânsito.

REFERÊNCIAS

1. Brasil. Medida Provisória nº 927, de 22 de março de 2020. *Diário Oficial da União* [Internet]. 2020 Mar 22 [acesso 2020 Jul 20]. Disponível em: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-927-de-22-de-marco-de-2020-249098775

2. Brasil. Ministério da Saúde. Portaria nº 373, de 27 de fevereiro de 2002. Aprova a Norma Operacional da Assistência à Saúde – NOAS-SUS 01/2002. *Diário Oficial da União*. 2020 Fev 28;89(40E):52.

3. Brasil. Ministério de Estado do Trabalho e Emprego. Portaria nº 1510, de 21 de agosto de 2009. *Diário Oficial da União* [Internet]. 2009 Ago 25 [acesso 2020 Jul 21]. Disponível em: http://www.trtsp.jus.br/geral/tribunal2/ORGAOS/MTE/Portaria/P1510_09.html

4. Brasil. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações* [Internet]. Brasília (DF): GSI; 2014[acesso 2020 Jul 21]. Disponível em: https://livrozilla.com/doc/568829/norma-complementar-n%C2%BA-07-in01-dsic-gsipr

5. Harmonson R. *Two factor authentication using FreeRADIUS with SSSD (FreeIPA or Active Directory) and Google Authenticator on CentOS 7* [Internet]. San Francisco: GitHub; 2017 [acesso 2020 Jun 20]. Disponível em: https://rharmonson.github.io/2factorcos7.html

Recebido: 27 jul 2020
Aceito: 6 ago 2020