CARTILHA

IMPLEMENTAÇÃO DO HOME OFFICE

PERSPECTIVAS JURÍDICA E DE SEGURANÇA DA INFORMAÇÃO

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

ICTS protiviti®

APRESENTAÇÃO

Com a declaração da pandemia pela Organização Mundial da Saúde, empresas de todos os portes tiveram que realizar a migração parcial ou integral de suas operações para o home office, como forma de garantir a continuidade dos seus negócios.

O modelo foi tão eficiente que se revelou um caminho sem volta. A crise sanitária ainda não terminou, mas já trouxe uma profunda mudança na cultura das organizações.

Como tudo isso aconteceu rapidamente, muitas empresas não tiveram tempo hábil para fazer uma avaliação criteriosa dos riscos legais e de segurança da informação envolvidos no trabalho fora das dependências corporativas.

Porém, com a consolidação do home office como uma realidade que se perpetuará, é chegado o momento de identificar tais riscos e adotar medidas para mitigá-los.

O objetivo desta cartilha é ajudar as empresas a seguirem com o home office de forma segura, pautadas nas melhores práticas jurídicas e de segurança da informação.

O material foi elaborado sob duas perspectivas. A jurídica, que contou com a contribuição do Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados, cuja missão é apoiar os clientes na evolução digital, com segurança jurídica e serviços especializados. E a da segurança da informação, que teve a colaboração da ICTS Protiviti, reconhecida empresa de consultoria, auditoria e serviços em gestão de risco.

Por meio desta cartilha, visamos esclarecer pontos relevantes acerca do home office. Destacamos, no entanto, que a avaliação e decisão final sobre a forma de implementá-lo deve ser cuidadosamente analisada de acordo com as características de cada organização, estando o Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados e a ICTS Protiviti isentas de qualquer responsabilidade.

Atenciosamente,
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados | ICTS Protiviti

ÍNDICE

1. Minha empresa pretende manter as operações em home office. Qual o primeiro passo em busca de segurança?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

O primeiro passo é a formalização contratual do home office, com o aditamento do Contrato de Trabalho vigente para documentar a realização das atividades fora das dependências da empresa, em situação esporádica ou regular, com a manutenção ou alteração da jornada de trabalho cumprida anteriormente no escritório e, em especial, com a definição da responsabilidade pela aquisição, manutenção e fornecimento dos recursos de Tecnologia de Informação necessários para a prestação dos serviços em casa. O aditamento deve incluir ainda disposições claras sobre o reembolso das despesas arcadas pelo empregado.

Vale lembrar que a legislação trabalhista não menciona a expressão home office, adotando termos como "teletrabalho", "trabalho remoto" ou "trabalho a distância", que não necessariamente são considerados sinônimos para fins legais, o que pode gerar consequências distintas sobre os direitos dos trabalhadores. A depender do modelo escolhido, os empregados usufruirão de direitos idênticos aos que contavam enquanto trabalhando no escritório ou usufruirão de direitos diferentes.

Assim, é necessário definir os detalhes do modelo de trabalho externo que a empresa pretende implementar, avaliar o regime legal no qual se enquadra e apurar quais serão os direitos correspondentes. Tudo isso considerando a premissa da vedação à alteração contratual que possa resultar em prejuízos ao empregado (art. 468).

Por fim, é importante lembrar que a Medida Provisória n.º 927/2020, que definiu medidas trabalhistas para o enfrentamento da emergência de saúde decorrente do COVID-19, alterou temporariamente as regras previstas na CLT para impor ao empregador as seguintes condições durante o estado de calamidade pública:

(i) a obrigação de notificar o empregado sobre a alteração do regime de trabalho presencial para o teletrabalho, trabalho remoto ou trabalho a distância, com antecedência de 48 horas, por escrito ou por meio eletrônico;

(ii) dispensar a necessidade de aditamento prévio do Contrato de Trabalho, cuja formalização deve ocorrer no prazo de 30 dias, contados da data da mudança do regime de trabalho; e

(iii) o aditamento deve estabelecer a definição da responsabilidade pela aquisição, manutenção e fornecimento de equipamentos tecnológicos e infraestrutura necessária para a prestação dos serviços fora das dependências do empregador e as disposições relativas ao reembolso de despesas arcadas pelo empregado (art. 4º e incisos).

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

Para agir com segurança técnica, é fundamental garantir a definição da infraestrutura de forma cuidadosa, já que esta será utilizada pelos colaboradores no trabalho remoto. Dessa forma, o mais adequado seria disponibilizar equipamentos corporativos, como filtros de tela, sistemas operacionais atualizados e programas de antivírus.

Além disso, a empresa pode aplicar processos de mapeamento das ameaças, como mitigação dos riscos e execução das atividades corretivas. Tudo isso com foco na infraestrutura e no objetivo principal de torná-la preparada para enfrentar tentativas de ataques. Fazer revisões das proteções de rede, permitir acesso somente via VPN e pela nuvem (Cloud) e realizar testes de invasões na VPN são importantes medidas.

Assim, é válido que as políticas de segurança da informação sejam constantemente revisadas e atualizadas pela equipe responsável.

Por fim, é necessário que o acesso via USB seja bloqueado para uso indiscriminado de pendrives ou outros dispositivos, de forma a garantir maior segurança na rede com um monitoramento dos logs eficazes.

2. Quem deve prover a infraestrutura de tecnologia para viabilizar o home office?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

Essa é uma questão sensível, pois a CLT não disciplina com clareza quem é o responsável pela obrigação de prover a infraestrutura de tecnologia (hardware, software e conexão à Internet) para o home office.

Especificamente para o teletrabalho, a redação deficitária da legislação leva a entender que empresa e empregado poderiam decidir por meio de livre negociação de que forma seria estabelecida a estrutura necessária para a implementação desse modelo (art. 75-D).

Porém, na prática, é pouco provável que a livre negociação seja considerada pela Justiça do Trabalho em caso de litígio, uma vez que a própria CLT adota o princípio da alteridade, consubstanciado na ideia de que os riscos da atividade econômica são assumidos pelo empregador. Assim não poderia haver transferência ao empregado de despesas relativas ao trabalho (art. 2º).

A Medida Provisória n.º 927/2020 estabeleceu que, durante o estado de calamidade pública, na hipótese de o empregado não possuir os equipamentos tecnológicos e a infraestrutura necessária e adequada à prestação do teletrabalho, trabalho remoto ou trabalho a distância, a empresa poderá fornecer os equipamentos em regime de comodato (empréstimo gratuito) e pagar pelos serviços de infraestrutura, sem que isso caracterize verba de natureza salarial (art. 4º, § 4º, inc. I).

Desse modo, o melhor cenário sob a perspectiva de segurança jurídica é a disponibilização pela empresa de toda a infraestrutura de Tecnologia da Informação para viabilizar o home office ao empregado, no modelo de comodato, arcando com as despesas de instalação e manutenção decorrentes.

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

A fim de garantir a proteção e a segurança dos dados da empresa, o ideal seria permitir apenas o uso de dispositivos corporativos, evitando aqueles de ordem pessoal, exceto em casos emergenciais ou realmente necessários. Tais questões devem ser delimitadas de forma clara na política de BYOD (Bring Your Own Device ou "Traga seu próprio dispositivo").

Para ambos os casos, algumas medidas de segurança podem ser providenciadas, tais como:

- Antes de serem entregues aos colaboradores, todos os dispositivos devem ter seus discos criptografados de acordo com o padrão homologado pela área de Segurança da Informação da empresa;

- Todo usuário deve receber um identificador (com login e senha) exclusivo e intransferível para ter acesso aos recursos de TI, além de permissão mínima para executar suas tarefas de trabalho;

- Os dispositivos devem ser entregues para os colaboradores após a aplicação das atualizações e políticas de segurança homologadas pela área de Segurança da Informação;

- Os dispositivos devem ser conectados a um domínio válido pela empresa, a fim de garantir que cada uma das diretrizes de segurança sejam aplicadas; e

- O uso de filtro de privacidade para evitar que pessoas estranhas à organização (mesmo familiares ou amigos) tenham acesso às informações nas telas de monitores.

3. Quais preocupações devo ter com a segurança da informação?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

As melhores práticas de governança de Segurança da Informação são baseadas na implementação de controles internos, que abarcam medidas de ordem técnica e administrativa. Assim, as preocupações sob a perspectiva jurídica devem se concentrar em dois pontos:

(i) Garantir que os controles tecnológicos atentem para os limites da privacidade do empregado; e

(ii) Implementar políticas com regras claras para o home office.

A orientação do Tribunal Superior do Trabalho é no seguinte sentido:

(i) Recursos de Tecnologia da Informação de propriedade corporativa utilizados como ferramentas de trabalho podem ser monitorados pela empresa, desde que afastada a expectativa de privacidade por parte do empregado, um vez que este foi previamente informado de forma transparente a respeito da existência de controles; e

(ii) Recursos de Tecnologia da Informação de propriedade do empregado, ainda que utilizados como ferramentas de trabalho, não podem ser monitorados pela empresa, sob pena de violar a privacidade do empregado.

Considerando que as empresas adotam modelos diversos, os pontos de atenção são diferentes para cada modelo:

CENÁRIO 01

A EMPRESA PROVÊ TODA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO AO EMPREGADO PARA VIABILIZAR O HOME OFFICE.

Considerando que todas as ferramentas de trabalho (hardware, software e conexão à Internet) são de propriedade da empresa, os controles de segurança da informação aplicáveis aos recursos tecnológicos anteriormente existentes no ambiente de trabalho poderão também ser implementados no modelo home office. Para tanto, é necessário implementar Políticas Corporativas com regras claras a respeito de que tais controles existem também no trabalho realizado dentro da residência do empregado.

CENÁRIO 02

A EMPRESA PROVÊ PARTE DA INFRAESTRUTURA DE TECNOLOGIA PARA VIABILIZAR O HOME OFFICE E O EMPREGADO PROVÊ A OUTRA PARTE.

Considerando que parte dos recursos de Tecnologia da Informação são de propriedade do empregado, controles de segurança da informação poderão sofrer limitações. Essa prática é conhecida como BYOD (Bring Your Own Device) e normalmente envolve o uso de dispositivos pessoais como notebook, tablet e smartphone para fins profissionais. Embora proporcione praticidade, impõe o desafio de garantir segurança da informação em uma infraestrutura que não é preparada para isso. Nesse caso, a segurança jurídica dependeria da instalação de tecnologias de conteinerização, criando-se um espaço corporativo dentro do hardware do empregado, com a adoção de todos os protocolos de segurança necessários. Os controles de segurança da informação, portanto, seriam restritos ao contêiner criado, preservando-se a privacidade. Para legitimar a prática, seria necessária a implementação de uma Política de BYOD que estabeleça regras claras a respeito dos controles efetuados e seus respectivos limites, bem como a obtenção de autorização do empregado para instalar as tecnologias aqui tratadas em dispositivos de sua propriedade.

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

Entre as principais preocupações de segurança da informação acerca do home office, está o uso das redes de Wi-fi residenciais. Além disso, é preciso assegurar que o roteador não esteja mais configurado com a senha padrão do fabricante.

Já em redes públicas, o uso deve ser evitado. Se a conectividade não for necessária naquele momento, a recomendação é que se desliguem o Wi-fi, o Bluetooth ou qualquer outra conexão.

Também é sensível para a segurança da informação o uso de equipamentos corporativos por outras pessoas alheias à empresa, como familiares ou amigos do empregado. Dessa forma, ele acaba sendo responsável pelo uso correto e seguro dos recursos de informação que foram colocados à sua disposição. Portanto, cabe a ele zelar pela integridade física e lógica, bem como pelos controles de acesso que lhe horam designados em contrato.

Por fim, é fundamental reforçar a importância de possuir senhas complexas, além das boas práticas, como o costume de redefinir senhas com frequência.

4. Posso condicionar o trabalho a condições técnicas mínimas de segurança da informação? E se o empregado não tiver condição?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

Como dito anteriormente, a CLT adota o princípio da alteridade, consubstanciado na ideia de que os riscos da atividade econômica são assumidos pelo empregador. Assim, não poderia haver transferência de despesas relativas à Segurança da Informação ao empregado (art. 2º).

A Medida Provisória n.º 927/2020 estabeleceu que, durante o estado de calamidade pública, se o empregado não possuir os equipamentos tecnológicos e a infraestrutura necessários e adequados para a prestação do teletrabalho e a empresa também não puder fornecê-los no modelo de comodato, o período da jornada normal de trabalho será computado como tempo de trabalho à disposição do empregador.

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

A infraestrutura deverá ser fornecida pela empresa, para que esta assegure as condições mínimas de segurança da informação. No entanto, quando não for possível fornecer toda ou qualquer infraestrutura, é importante orientar os colaboradores no sentido de garantir a segurança das informações por meio das medidas de proteção já citadas nesta cartilha.

5. A empresa pode controlar o cumprimento da jornada de trabalho por meio de ferramentas de tecnologia?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

A CLT não distingue o trabalho realizado no escritório da empresa do trabalho realizado na residência do empregado ou a distância, equiparando as ferramentas informatizadas de controle e supervisão a ferramentas de controles pessoais (art. 6º, Parágrafo Único).

Na prática, quer dizer que a empresa pode usar a tecnologia para controlar o cumprimento da jornada de trabalho. A consequência é que, no caso da implementação desse tipo de controle, o empregado poderá ter direito à remuneração por hora extra, mesmo trabalhando em home office.

Caso não haja qualquer controle de jornada, o empregado em tese não fará jus a esse direito, pois poderia restar caracterizado o regime de teletrabalho, exceção estabelecida pela CLT (art. 62, III).

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

Hoje, é possível controlar o cumprimento da jornada por meio de pontos eletrônicos, seja no desktop ou por aplicativos no celular. Isso permite ao empregador fazer o controle de login com base no horário e também bloquear o acesso do usuário fora do horário estipulado em sua jornada de trabalho.

Porém, este controle é muito restritivo e pode causar impactos nas operações, visto que o usuário não poderá tomar ações fora de seu horário comercial.

6. Como preparar meu empregado para essa nova realidade digital?

PERSPECTIVA JURÍDICA DO OPICE BLUM:

Invariavelmente, as organizações têm colaboradores de diferentes graus de familiaridade com a tecnologia. Lado a lado, trabalham imigrantes virtuais - nascidos em um mundo analógico e que só tiveram contato com a tecnologia na faculdade ou nas primeiras experiências profissionais - e nativos digitais - já nasceram inseridos no contexto virtual e são extremamente hábeis no uso das novas tecnologias.

No entanto, é provável que ambos os grupos nunca tenham recebido educação digital! Afinal, somos a única geração da humanidade que viveu em um mundo totalmente analógico e agora enfrenta o desafio de viver em um mundo totalmente digital.

É fundamental que a empresa, além de estabelecer Políticas Corporativas sobre Ética, Segurança da Informação, Proteção de Dados Pessoais e Home Office, crie programas para conscientizar, instruir e ensinar todos os empregados sobre esses temas. A educação é pré-requisito para que se concretize a utilização da infraestrutura de tecnologia de forma segura.

PERSPECTIVA DA ICTS SOBRE SEGURANÇA DA INFORMAÇÃO:

É importante que as definições e regras do trabalho remoto estejam definidas de forma clara na Política de Segurança da Informação e sejam previamente divulgadas para todos os colaboradores da empresa, cujas equipes de TI poderão assegurar a acessibilidade dos mesmos sempre que necessário.

A empresa pode inclusive aumentar a quantidade de sessões de treinamento na área de Segurança da Informação por meio de campanhas e novos métodos de aprendizado, importantes para o cenário atual.

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Presentes no mercado desde 1997, orientamos nossos clientes na evolução digital, com segurança jurídica e serviços especializados.

Somos pioneiros em Direito Digital no país e referência também em Proteção de Dados, Tecnologia da Informação, Propriedade Intelectual, entre outras áreas.

Nossa atuação é reconhecida no Brasil e no exterior por diretórios jurídicos como Chambers & Partners Latin America, Who's Who Legal, Legal 500, Best Lawyers, Leaders League e Análise Advocacia.

Para saber mais sobre o Opice Blum e nossas frente de atuação, visite www.opiceblum.com.br.

SÓCIOS:

José Roberto Opice Blum
Renato Opice Blum
Marcos Bruno
Juliana Abrusio
Rony Vainzof
Caio Lima
Camilla Jimene

IDEALIZAÇÃO :

Renato Opice Blum
Rony Vainzof

AUTORIA:

Rony Vainzof
Camilla Jimene
Ana Maria Roncaglia

REALIZAÇÃO:

Lara Silbiger
Paola Cosentino

Alameda Joaquim Eugênio de Lima, 680 - 1º andar, Jardim Paulista, São Paulo SP - CEP: 01403001
opiceblum.com.br | contato@opiceblum.com.br | +55 11 2189-0061
@opiceblum

A **ICTS** é uma empresa brasileira de consultoria, auditoria, tecnologia e serviços, com ampla atuação nos segmentos de gestão de riscos, ética, compliance e segurança. Propicia aos seus clientes proteção no presente e confiança no futuro.

Opera no mercado com duas marcas: a ICTS Protiviti, que combina uma plataforma tecnológica de serviços especializados - canal de denúncias, diligência de terceiros, monitoramento de fraudes e de comportamentos antiéticos, e treinamentos on-line, ao alcance global e o conhecimento e inovação em gestão de riscos, compliance, proteção e privacidade de dados, auditoria interna e investigação empresarial da Protiviti; e a ICTS Security, que oferece consultoria e gestão de serviços de segurança empresarial, pessoal e condominial, com enfoque preventivo e aporte de inteligência e tecnologias de ponta.

SÓCIOS:

André Cilurzo

Heloisa Macari

Jefferson Kiyohara

Matheus Jacyntho

Maurico Fiss

Rua James Joule, 65, 5º andar • Cidade Monções • São Paulo • SP • Brasil • CEP: 04576-080
www.icts.com.br | contato@icts.com.br | +55 11 3809-2681

@ictsprotiviti @icts-protiviti