ENJOY SAFER TECHNOLOGY™

PARA COLABORADORES

GUIA DE

Trabalho a distância

Introdução

Com o crescimento das tecnologias da informação e comunicação, cada vez mais colaboradores têm a possibilidade de se conectar aos serviços da empresa de qualquer lugar ou dispositivo; ou mesmo trabalhar remotamente para empresas que não estão localizadas no seu país de residência.

As vantagens dessa nova tendência são claras; os funcionários economizam tempo e dinheiro em viagens, podem trabalhar mais descontraídos e gerenciar melhor seu trabalho; para a empresa, isso significa aumento da produtividade e redução dos custos de infraestrutura.

No entanto, essa modalidade de trabalho traz consigo uma série de desafios para garantir a confidencialidade, a integridade e a disponibilidade das informações. As medidas de segurança normalmente aplicadas no domínio da empresa não são suficientes para proteger os dados manipulados fora dela. Portanto, o controle do acesso e uso das informações se torna cada vez mais complicado. Isso torna a responsabilidade de cuidar das informações cada vez mais um compromisso do trabalhador.

O objetivo deste documento é fornecer informações aos colaboradores sobre como proteger as informações, especialmente quando estão trabalhando remotamente.

Índice

O que é o trabalho a distância?

O trabalho a distância é uma modalidade de trabalho que **consiste em realizar as tarefas habituais de um lugar que não as instalações da empresa, utilizando como suporte diferentes tecnologias de comunicação.**

Existem muitas atividades que não necessariamente devem ser executadas em um escritório, e tampouco requerem a presença do trabalhador no seu posto de trabalho, pois podem sem realizadas em um local diferente. Atualmente, a incorporação de novas formas de comunicação nos permite facilitar as tarefas e executar o trabalho de maneira satisfatória independentemente do local em que é realizado.

Fazer "Home Office" não significa, obrigatoriamente, trabalhar do conforto de casa, como também se refere à toda forma de trabalho remoto, sempre e quando as ferramentas necessárias para o realizar estiverem disponíveis. Isso significa que trabalhar da casa de um amigo, em um bar, uma biblioteca, até mesmo de um hotel ou aeroporto durante uma viagem de negócios também constituem formas de trabalho a distância.

Essa metodologia tampouco se limita aos funcionários com relações de trabalho formal, muito pelo contrário. Diversos são os profissionais autônomos e independentes que trabalham por meio de conexão remota para diferentes clientes, aproveitando as vantagens das telecomunicações.

Portanto, sempre que um funcionário, formal ou autônomo, realizar suas tarefas habituais fora do endereço do empregador (ou do cliente) utilizando tecnologias de comunicação, isso é chamado de trabalho a distância.

Riscos e ameaças

Além dos benefícios do trabalho a distância, essa metodologia também implica considerar certos riscos, os quais habitualmente são mitigados dentro das instalações do empregador, mas se situam fora de alcance quando as informações são acessadas remotamente.

Esses riscos podem ocorrer devido a situações intencionais ou acidentais, bem como comprometer a segurança das informações, tanto do trabalhador como da empresa.

Podemos classificá-los segundo o comprometimento de confidencialidade, integridade e disponibilidade das informações.

Confidencialidade

Riscos que podem provocar que um terceiro não autorizado, seja um indivíduo ou processo, acesse informações privadas. Alguns exemplos são:

- Conectar-se à uma rede Wi-Fi, desconhecida ou insegura, que pode provocar que um terceiro também se conecte às informações recebidas ou enviadas do dispositivo.
- Se um dispositivo for roubado, as informações nele contidas também o são, podendo ficar expostas a um ofensor.

Integridade

Situações em que um terceiro não autorizado, sejam um processo ou um indivíduo, poderia alterar as informações.

- Um código malicioso que infecta um dispositivo pode modificar tanto as informações nele localizadas como aquelas às quais o dispositivo ou usuário infectados tenham acesso.
- Em uma conexão remota insegura, um indivíduo poderia alterar os certificados e assinaturas digitais e falsificar uma identidade.

Disponibilidade

Ameaças que poderiam fazer com que um sistema não esteja mais acessível ou utilizável quando necessário.

- As informações localizadas em um dispositivo, ou até mesmo o dispositivo em si, podem ser criptografadas por um código malicioso que infectou o dispositivo e, assim, ficar inutilizada.
- O acesso remoto às informações ou aos serviços localizados em servidores da empresa pode ser interrompido se a conexão estiver instável.

Dentro do domínio de uma empresa, esses riscos costumam ser mitigados ou controlados por diferentes departamentos, aplicando diversas medidas de segurança, **mas uma vez fora desse ambiente protegido passa a ser de responsabilidade do trabalhador mitigá-los ou reduzi-los.**

Política corporativa

Antes de entrar em assuntos técnicos, ferramentas de trabalho ou configurações, é fundamental estabelecer um marco normativo que padronize as condições e procedimentos mediante os quais o trabalho a distância será desenvolvido.

A empresa deve fornecer aos colaboradores uma política de trabalho a distância clara, que aborde pontos como:

- Quem terá acesso a essa modalidade e em quais circunstâncias.
- Procedimento de conexão remota.
- Dispositivos e ferramentas que serão utilizados no cumprimento das tarefas.
- Como lidar com as informações fora das instalações da empresa.
- Qual é o procedimento ou contato em caso de necessidade de assistência técnica.
- Responsabilidades e obrigações do teletrabalhador em questões de segurança da informação.

É crucial, tanto para o trabalhador como para o empregador, que as regras sejam claras. Antes de começar a trabalhar de maneira remota, de se conectar à rede da empresa ou de utilizar diferentes dispositivos para acessar informações, é importante que o trabalhador conheça e entenda a política de trabalho. É necessário que tenha claro quais são suas responsabilidades no que concerne à segurança, se pode ou não utilizar dispositivos próprios e, caso possa, quais cuidados deve ter, de que maneira pode usar os serviços de comunicação da empresa e, acima de tudo, quais são as medidas de segurança estabelecidas e quais as ferramentas disponíveis para cumprir essas medidas.

Quer sejam funcionários formais ou profissionais autônomos lidando com as informações dos clientes, é imprescindível, em todos os casos, conhecer a política de trabalho a distância ou de acesso remoto para que sempre sigam **as diretrizes de segurança do negócio.**

Ferramentas de trabalho a distância para o funcionário

Ao trabalhar remotamente, é necessário ter ferramentas que permitam portabilidade e conectividade aos serviços e sistemas do empregador. Essas ferramentas, físicas e digitais, são variadas e cada vez mais populares. A seguir, analisaremos as mais comuns e explicaremos como protegê-las.

Dispositivos móveis

Entre as ferramentas que possibilitam o trabalho a distância, as mais comuns são os dispositivos móveis. Quer sejam ser laptops, tablets ou telefones celulares, esses dispositivos facilitam a mobilidade e permitem que você execute diferentes tarefas, no conforto da sua casa, em um meio de transporte, durante uma viagem ou em qualquer outro local à distância.

Por meio desses dispositivos, informações confidenciais são acessadas e armazenadas, por isso é importante levar em consideração os riscos associados ao seu uso e, principalmente, à sua perda ou roubo.

Senha de acesso ao dispositivo

Ao trabalhar de um lugar público ou um escritório compartilhado com outras pessoas desconhecidas, é importante **nunca deixar o dispositivo sem supervisão**. Além disso, caso não seja utilizado por um período, deve-se sempre bloqueá-lo com uma senha, inclusive sendo importante que ele se bloqueie automaticamente por inatividade. Dessa forma, evita-se que em um momento de descuido um terceiro possa acessar facilmente as informações do dispositivo.

Proteção Antirroubo

No caso de perda ou roubo de um dispositivo, há ferramentas que previnem que as informações ou os acessos armazenados sejam acessados por terceiros, bem como também podem ajudar a localizá-lo e recuperá-lo.

A função de proteção antirroubo permite rastrear o dispositivo por meio de sua função GPS para tentar recuperá-lo, assim como enviar mensagens ao dispositivo, que podem ser lidas pela pessoa que o tenha encontrado.

Além disso, é possível **monitorar a atividade** do dispositivo, detectar ações estranhas e, inclusive, ver fotografias capturadas com a câmera ou da mesma tela. Tudo isso é feito protegendo as contas e informações do usuário para que não possam ser acessadas por quem estiver com o dispositivo.

Por último, essa funcionalidade permite realizar certas **ações de prevenção** no dispositivo de maneira remota, habitualmente mediante o envio de um SMS, como por exemplo **bloqueá-lo**, **deletá-lo** ou até **eliminar todos os dados** armazenados e restaurar a configuração de fábrica.

É altamente recomendável ativar esse tipo de proteção, tanto em dispositivos móveis pessoais como corporativos.

Dispositivos de Armazenamento

Dentro dos dispositivos móveis, muitas informações são enviadas, além de arquivos e certificados pessoais e informações de sessão das diferentes contas. Essas informações são armazenadas nos discos e memórias de diferentes dispositivos, como o disco de um laptop, a memória de um celular ou até mesmo um pendrive.

No caso de perda de qualquer dispositivo, as informações dentro dele também serão perdidas, por isso é importante levar em consideração as seguintes tecnologias e medidas de segurança:

Criptografia

A criptografia é uma medida de segurança muito utilizada para proteger os dados localizados em um dispositivo. Ela consiste em alterar as informações de acordo com um padrão estabelecido por uma chave, de tal forma que os dados somente sejam de conhecimento de quem possui essa chave.

Ao criptografar as informações, elas se tornam ilegíveis, e é por isso que se o dispositivo for roubado, cair nas mãos de terceiros ou, inclusive, for infectado por um código malicioso que tenta roubar os arquivos, a única informação que irá aparecer será em forma de caracteres sem sentido.

Apesar do que geralmente se acredita, o uso de ferramentas de criptografia é realmente eficiente e fácil de fazer para qualquer usuário. Basta saber quais informações queremos proteger e configurar a ferramenta de criptografia utilizada com uma chave forte e segura. **Para mais informações, recomendamos verificar o Guia de Criptografia.**

Backup

Neste guia, falamos sobre como proteger as informações para que elas não sejam acessadas ou modificadas por terceiros não autorizados, mesmo que um dispositivo seja perdido. No entanto, também é importante pensar em como recuperar as informações perdidas para continuar com as tarefas usuais.

Nesse sentido, é necessário fazer backup de todos os arquivos que não podem ser recuperados facilmente. Por exemplo, documentos de autoria própria, relatórios, pesquisas, planilhas e apresentações; até mesmo fotografias e documentos pessoais.

Os tipos de backup que podem ser usados são diversos e se deve avaliar qual deles se adapta às necessidades de cada usuário. **Para mais informações, recomendamos a leitura do Guia de Backup.**

Conectividade

Atualmente, a conectividade se tornou um serviço básico para o desenvolvimento da vida cotidiana e é possível acessar a Internet a partir de vários locais e conexões, inclusive de graça.

Assim como essa tecnologia possibilita a realização do trabalho a distância, também pode ser a porta de entrada para algumas ameaças se não estiver configurada corretamente ou se um intruso a ela se conectar. É por isso que é sempre preferível usar redes sem fio seguras para evitar riscos.

Redes Públicas/Redes Privadas

A maioria das empresas possui redes Wi-Fi privadas que protegem os dados que trafegam pela rede e garantem uma navegação segura aos usuários. No entanto, quando a conexão for remota, é necessário um ponto de acesso à Internet, que geralmente não possui os mesmos controles ou medidas da rede interna da empresa.

Quais são as redes sem fio seguras?

São aqueles em que várias medidas de segurança foram aplicadas para impedir a conexão de terceiros não autorizados. Dentro dessas medidas de segurança, existe uma que é fundamental e que pode ser facilmente identificada: **a senha**. Uma rede sem senha ou com uma senha fraca pode ser facilmente acessada por terceiros. Dessa forma, uma pessoa que possua os conhecimentos necessários poderia, sem problemas, obter uma senha com criptografia WEP muito mais facilmente do que uma senha **criptografada em WPA ou WPA2**, sendo esta última a mais segura e recomendada.
No caso de redes domésticas, também é importante que o **roteador Wi-Fi não possa ser acessado de fora** e conte com uma chave de administrador forte e difícil de adivinhar. Por último, é recomendável manter o firmware do roteador atualizado e monitorar os dispositivos conectados à rede.
Por outro lado, também existem as redes públicas, que são muito úteis quando se trabalha em um bar, aeroporto ou qualquer outro local público. Normalmente, são redes abertas oferecidas como um serviço adicional ao cliente. Essas conexões não possuem medidas restritivas de segurança e qualquer pessoa a elas conectada pode interceptar e até manipular o tráfego de outros dispositivos na rede. No caso de uma conexão nesse estilo, é necessário aplicar as configurações de segurança mais restritivas, especialmente em relação a arquivos compartilhados e acesso ao sistema. Se os controles de segurança relevantes não forem levados em consideração, é recomendável **evitar o uso de serviços que solicitem informações confidenciais em conexões sem fio públicas.**

É comum usar redes que não sejam nem da sua própria casa nem públicas, mas sim redes de terceiros, seja a de um hotel, a da casa de um amigo etc. Apesar de serem privadas, o usuário não conhece as outras pessoas conectadas à mesma rede, nem suas intenções. Portanto, as precauções utilizadas devem ser as mesmas para aquelas redes públicas, mesmo quando o administrador da rede for conhecido e de confiança.

VPN

As VPNs (Redes Privadas Virtuais) são conexões criptografadas utilizadas **para se conectar de maneira segura à uma rede privada conhecida**, por exemplo, a rede interna de uma empresa.

Embora existam protocolos diferentes para conexão via VPN, todos usam comunicações criptografadas, ou seja, os dados transmitidos são ilegíveis até que cheguem ao seu destino. Dessa forma, mesmo se forem interceptados por terceiros, essas pessoas não poderão ler ou usar os dados.

A maioria das empresas fornecem conexões VPN aos seus usuários para que eles possam acessar os serviços da rede interna de maneira remota.

Visto que essas conexões são criptografadas, é recomendável utilizá-las sempre que estiver conectado à uma rede pública ou insegura, pois irão evitar que as informações sejam interceptadas (ou se forem, irão torná-las inúteis).

Autenticação de dois fatores

A autenticação de dois fatores é um sistema que complementa a autenticação tradicional em serviços. Ou seja, além de exigir que um usuário e uma senha acessem um sistema ou serviço, também requer uma terceira informação, como um código de segurança, uma impressão digital ou qualquer outra informação adicional que o usuário tenha. Geralmente, um código gerado aleatoriamente é usado em um dispositivo, como um token ou um aplicativo no celular.

O objetivo da autenticação de dois fatores é proteger o acesso às contas e serviços do usuário se a sua senha for comprometida, seja por código malicioso, vazamento de informações ou engano. Independentemente do caso para o qual as credenciais da conta possam ter sido obtidas por um terceiro, ter uma autenticação de dois fatores habilitada evitará o acesso às informações sem o código correspondente.

Ao trabalhar remotamente, os riscos de que as credenciais possam ser obtidas por um atacante aumentam, principalmente ao se conectar a redes não seguras ou compartilhadas. Se um terceiro dado for necessário para efetuar login, o atacante não poderá acessar a conta, mesmo que obtenha o nome de usuário e a senha.

Antivírus e soluções de segurança

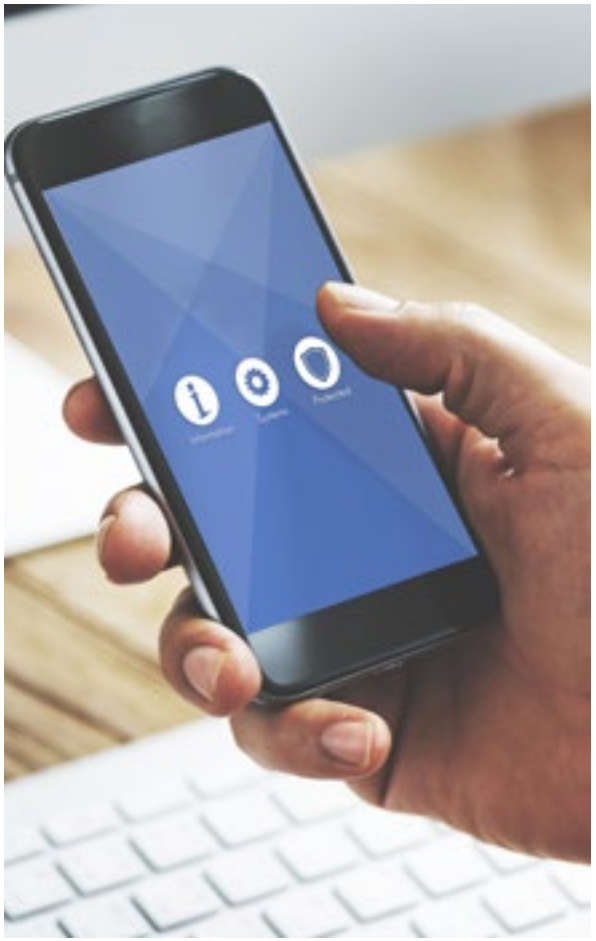
Ainda que o trabalhador tome todas as medidas indicadas neste guia, sempre existe a possibilidade de sofrer uma infecção por código malicioso, entrar em uma página fraudulenta ou comprometer informações na rede sem perceber. O motivo: nenhum dispositivo está isento de riscos.

Isso torna o complemento de todas as precauções com um sistema de **detecção proativo de ameaças essencial**, que se obtém por meio da **instalação de uma solução integral de segurança nos dispositivos**.

Estamos falando de uma solução abrangente e não apenas de um antivírus, pois atualmente não basta apenas detectar códigos maliciosos. Essas soluções possuem módulos diferentes que também detectam outros tipos de ameaças, como conexões inseguras, sites enganosos, pacotes malformados e outros sinais que podem indicar um possível risco.

Quando o trabalho remoto ocorre em empresas nas quais o usuário utiliza dispositivos corporativos para conectar e manipular informações, eles geralmente são protegidos por uma solução de segurança fornecida e gerenciada pela mesma empresa.
Sem dúvidas, **nos casos em que o trabalhador utiliza seus próprios dispositivos, essa medida de segurança é indispensável**. Não se deve contar apenas com uma solução de segurança em cada dispositivo, sejam de escritório ou móveis, nos quais informações confidenciais sejam manipuladas, como também **é necessário mantê-la atualizada** para prevenir novas ameaças.

No caso de dispositivos domésticos, especialmente aqueles usados por diferentes membros da família, os riscos de serem vítimas de uma ameaça aumentam, pois é difícil controlar o uso do dispositivo, os downloads que são feitos ou os sites que são acessados. Ter um produto protegido por uma empresa de segurança confiável com um histórico no mercado resolve esses problemas muito rapidamente, fornecendo uma camada de segurança a todos os usuários.



Suporte: a quem recorrer em caso de necessidade?

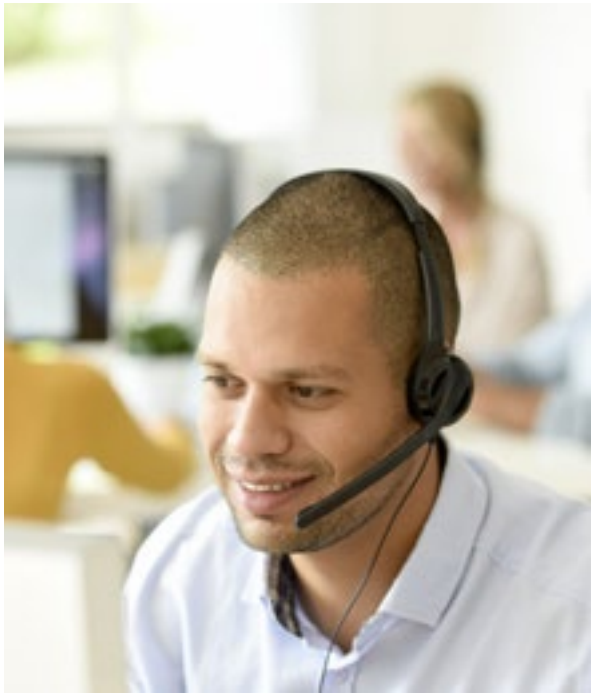
Conforme já mencionado ao longo deste guia, há vários problemas que precisam ser lembrados quando se trabalha remotamente, que são geralmente comuns ou resolvidos no ambiente do escritório. Uma dessas questões é o suporte ou assistência na resolução de um problema técnico.

Diferente do suporte no local de trabalho, onde geralmente é mais eficaz e simples resolver um problema, pois há acesso direto ao dispositivo, o suporte remoto geralmente traz algumas dificuldades e riscos que o trabalhador deve levar em consideração.
Por um lado, deve-se contar com os **contatos de quem pode ajudar no momento de relatar um problema** ou solicitar assistência. É importante tê-los sempre à mão e disponíveis em diversos dispositivos, para que, se um deles não puder ser acessado, as informações de contato também estejam disponíveis.
Isso também se aplica aos contatos para os quais relatar um incidente de segurança, como o roubo ou a perda de um dispositivo, em que **é de suma importância avisar assim que possível** ao empregador, para que os protocolos de segurança correspondentes possam ser executados e evitar que as informações sejam comprometidas.

Muitas empresas usam conexões de controle remoto de escritórios para dar ao técnico acesso ao dispositivo. Muitas dessas soluções são públicas e gratuitas, para que possam ser usadas por qualquer pessoa. Também existem truques diferentes que tentam fazer o usuário acreditar que está com um problema com o dispositivo e precisa de suporte, quando isso não é verdade.

De qualquer maneira, **é sempre importante entrar em contato com o suporte técnico autorizado do empregador** e se assegurar de quem, de fato, está acessando o dispositivo, **evitando dar acesso a pessoas desconhecidas ou de reputação duvidosa**. Também se recomenda prestar atenção nas ações que a pessoa encarregada pelo suporte executa no dispositivo, pois tendo ou não conhecimento técnico devemos garantir que as informações confidenciais não sejam acessadas nesse processo.

Como o suporte remoto pode não ser tão eficiente ou ter algumas limitações, também é aconselhável solicitar à empresa um guia de solução de problemas para os problemas mais comuns, para que possamos resolvê-los proativamente.



Boas práticas de segurança

Ao trabalhar remotamente, a segurança das informações permanece, em grande parte, nas mãos do usuário. Portanto, para mitigar os riscos que isso implica e proteger as informações, algumas boas práticas de segurança devem ser adotadas.

- Criptografar as informações dos dispositivos móveis.
- Utilizar uma solução de segurança e mantê-la atualizada.
- Manter todos os dispositivos atualizados, tanto o sistema operacional como os aplicativos.
- Utilizar, sempre que possível, redes Wi-Fi seguras, e configurar a rede doméstica sem fio de forma segura.
- Se você se conectar a uma rede pública ou compartilhada, use sempre uma VPN ou evite enviar informaçõnes confidenciais.
- Realizar backups periódicos das suas informações.
- Nunca deixar o dispositivo sem supervisão e protegê-lo com uma senha.
- Contar com uma proteção antirroubo.
- Utilizar autenticação de dois fatores para acessar contas críticas.
- Ter sempre à mão os contatos de suporte e, no caso de um incidente de segurança, relatá-lo assim que possível.
- Estar atento e informado a respeito de novos golpes e ameaças.

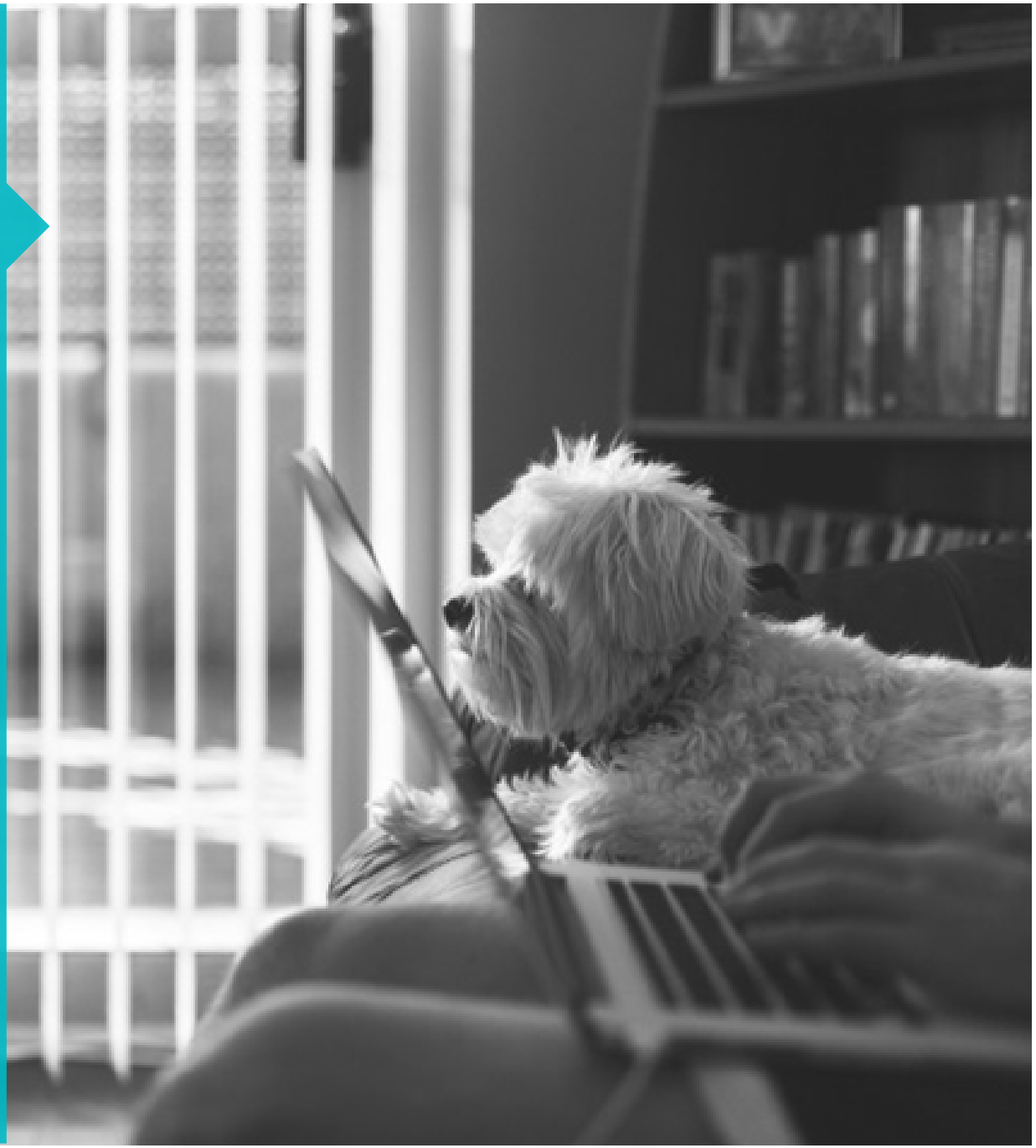
Conclusão

Neste guia, analisamos os riscos envolvidos no trabalho remoto e como se deve mudar a maneira pela qual a segurança é gerenciada para garantir que o acesso às informações seja feito com segurança.

Além disso, levando em conta novas tecnologias, como 4G, Wi-Fi em aviões e outros avanços em conectividade, o trabalho a distância e, principalmente, o acesso remoto a informações, é sem dúvida uma tendência crescente que as empresas implementem esse modelo, o qual os funcionários vão querer aproveitar.

À medida que as oportunidades e vantagens do trabalho a distância forem mais bem exploradas, o trabalhador se tornará uma parte fundamental da gestão para garantir a segurança das informações. E para enfrentar os novos desafios que possam surgir, as organizações devem ter políticas claras de gerenciamento de informações e ferramentas adequadas que permitam aos funcionários realizar suas atividades com segurança.

Embora o trabalho a distância não seja uma opção viável para todas as empresas, e mesmo naquelas em que se decida adotá-lo, talvez não consigam implementá-lo em todas as suas áreas. Para mudar a maneira de trabalhar na empresa é importante que todos os envolvidos sejam treinados para conhecer os riscos e como evitá-los e/ou combatê-los.



www.eset.com/br

/EsetBrasil @ESET_Brasil /company/eset-brasil