ENJOY SAFER TECHNOLOGY™

PARA EMPRESAS

GUIA DE Trabalho a distância

Introdução

O trabalho remoto ou trabalho a distância, se caracteriza pela realização do trabalho fora do escritório. Mesmo que ele seja geralmente associado ao home office, não está limitado somente ao trabalho em casa; isso pode ocorrer também em escritórios compartilhados ou qualquer espaço diferente do da empresa. Do mesmo modo, na maioria dos casos não existem horários definidos, mas sim tarefas e objetivos a serem cumpridos.

Sem dúvidas, essa metodologia ganhou força devido às possibilidades e o crescimento que a Internet oferece, especialmente quanto ao desenvolvimento de novas de tecnologias de comunicação integradas em sistemas com base na Nuvem.

Além disso, o trabalho a distância, dentre suas vantagens, é capaz de diminuir os custos corporativos. Isso se deve à portabilidade tecnológica que permite que os empregados sejam produtivos mesmo fora da empresa.

Isso obriga que as companhias levem em conta diversos panoramas, como a manipulação da informação corporativa em dispositivos que possam estar desprotegidos da forma adequada ou o acesso remoto a informações sensíveis. Esses casos, entre muitos outros, fazem com que as empresas se organizem de formas diferentes para gerenciar a segurança, minimizando os riscos associados a um ataque a informações mais críticas.

Índice

Mudanças de paradigma na gestão

Sem dúvidas, esse modo de trabalho implica em mudanças não só para o funcionário, mas também para os empregadores, já que devem considerar questões que vão desde onde o empregado acessa a informação, até a forma com que entra nos sistemas.

Por esse motivo, tudo que está relacionado com os equipamentos de trabalho, a responsabilidade e os custos devem estar definidos de forma clara antes de implementar uma forma de trabalho.

O mais comum é que o empregador proporcione e mantenha os equipamentos necessários para o trabalho regular, no entanto, também pode acontecer do funcionário utilizar seu próprio equipamento.

Independente do modo escolhido, a empresa deve considerar oferecer ao empregado um suporte técnico para que ele possa desenvolver suas tarefas sem nenhum problema.

Nesse sentido, a empresa deverá prestar muita atenção na forma como seus empregados se conectam às redes corporativas e públicas para administrar a informação, em detrimento da preocupação que antes se tinha devido à infraestrutura física. A adoção de metodologias de trabalho a distância significa uma transformação na forma de gestão de segurança dos dados em uma ampla variedade de dispositivos, aplicativos e sistemas operacionais.

Esse modo de trabalho implica em mudanças não só para o funcionário, mas também para os empregadores, já que devem considerar questões que vão desde onde o empregado acessa a informação, até a forma com que entra nos sistemas.

Desafios e oportunidades

Sem dúvidas, o trabalho a distância oferece oportunidades para aumentar a produtividade devido à implantação do trabalho com objetivos de menos custos ao diminuir a infraestrutura necessária e utilizando novas tecnologias que agilizem as tarefas dos empregados.

No entanto, esse método também implica em desafios e riscos que devem ser levados em consideração para implementar medidas de controle adequadas, já que se você não as estabelece, isso pode abrir brechas de segurança, dar chance de infecções com códigos maliciosos ou acessos não autorizados sobre informações privilegiadas.

Além de pensar nos benefícios econômicos e operacionais, as empresas devem levar em consideração os comportamentos e dispositivos de toda a equipe de colaboradores para tomar as medidas de controle adequadas e, assim, garantir que a informação permanecerá protegida.

Além do perímetro

Ao permitir que os funcionários acessem e manipulem informações fora do ambiente corporativo, a fronteira de complicações de segurança se amplia. Portanto, para administrar essa questão é necessário ir além do perímetro tradicional, que costumava se estender até o firewall da empresa.

Pensar em ameaças à informação nesse novo contexto, nos faz pensar em outros tipos de riscos que em um ambiente fora do perímetro corporativo possuem uma maior probabilidade de acontecer. Consequentemente, é necessário identificar as vulnerabilidades que são geradas e quais ameaças podem se aproveitar delas.

Vejamos algumas das que devem ser consideradas:

VULNERABILIDADES	AMEAÇAS
Senhas fracas	Perda de dispositivos
Ausência de soluções de segurança	Infecções por códigos maliciosos
Conexão a partir de redes desprotegidas	Execução de exploits
Dispositivos com informação não criptografada	Danos aos equipamentos
Falta de backups da informação	Truques baseados em egenharia social
Falta de atualizações de sistemas e dispositivos	

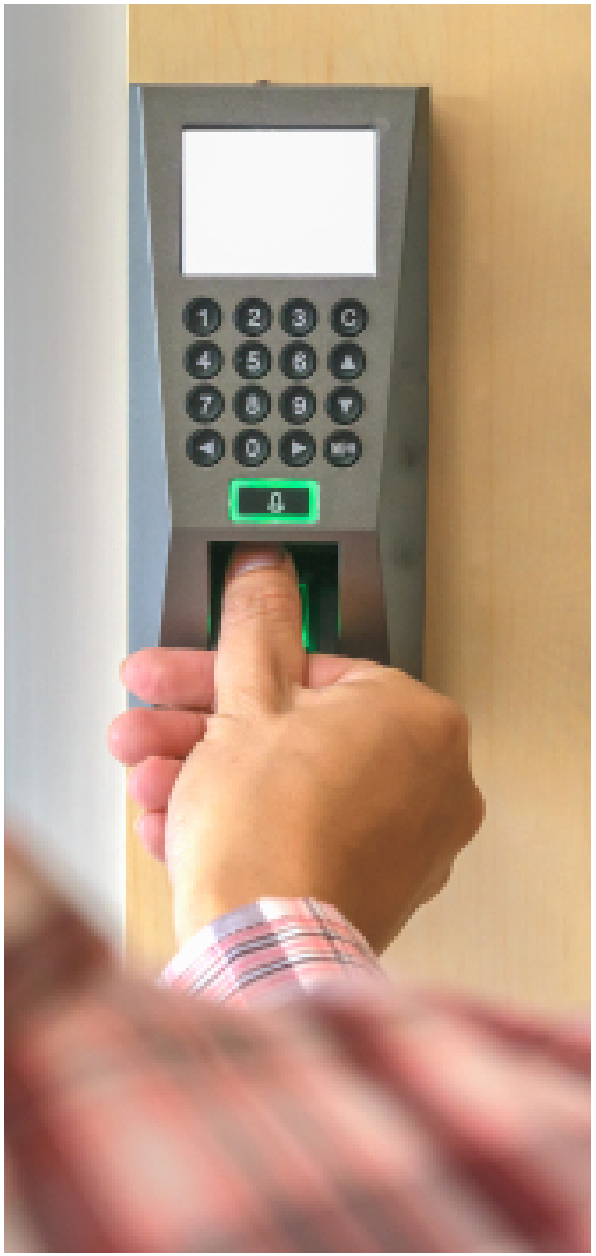
Gerenciando os riscos

O gerenciamento de riscos deve estar focado em implementar os controles adequados para corrigir as vulnerabilidades ou evitar que um incidente ocorra.

O primeiro passo que uma empresa deve dar antes de implementar uma política desse tipo é a classificação da informação com o objetivo de estabelecer, por exemplo, quais são os dados sensíveis que requerem um maior nível de proteção; quais informações podem ser acessadas a partir de dispositivos pessoais; quais podem ser acessadas fora da rede da empresa; e quais devem ter seu acesso completamente restringido.

Se a empresa possui um ponto de partida claro, é possível determinar quais são os riscos que possuem uma maior probabilidade de acontecer ou que podem ter um maior impacto, e a partir disso, determinar as medidas de controle mais adequadas para garantir a segurança da informação, tanto do tipo tecnológico como do de gestão.

A empresa primeiro deve classificar a informação para estabelecer quais dados devem ser de fácil acesso e quais devem possuir níveis de proteção maiores.



Por onde começar a identificar os riscos

Acessos a informações sensíveis a partir de ambientes não confiáveis

É necessário considerar o panorama no qual o funcionário acessa os sistemas corporativos a partir de redes Wi-Fi públicas ou a partir de dispositivos que se encontram desprotegidos.

Permissões de usuário no sistema

Se o funcionário trabalha a partir de seu próprio computador, pode ser que utilize um perfil de administrador. Portanto, não é posível controlar o que se instala ou que acessos adicionais se dão ao dispositivo.

Equipamento corporativo para uso pessoal

Quando a empresa oferece um computador ao funcionário para realizar o trabalho a distância, ele é capaz de utilizar esse equipamento para realizar atividades pessoais, portanto é necessário considerar esse tipo de uso e os inconvenientes que isso poderia causar com relação à informação corporativa do equipamento e seu respectivo acesso à rede da empresa.

Backup da informação

As tarefas de backup de informações importantes podem se tornar complicadas caso não se tenha em mente que muitos dos dados utilizados pelo funcionário podem estar armazenados de maneira local, ou seja, fora das atividades de backup. Isso é um grande problema se o equipamento não se encontra conectado às redes correspondentes no período programado.

Sistemas de autenticação fracos

Deixar uma autenticação única para acessar sistemas da empresa com um senha é a opção menos recomendada. É importante pensar em outras formas de autenticação que possam adicionar mais camadas de proteção.

Falta de políticas de segurança

Tanto o empregado como a empresa devem saber de maneira clara o que podem fazer e como devem realizar as tarefas. Se isso não está claro, se torna um elo fraco na cadeia de segurança.

Controle de dados corporativos e virtualização

Uma das melhores alternativas que as empresas possuem para aplicar um esquema de trabalho é a virtualização de seus ambientes. Com essa abordagem é possível obter um maior controle dos dados mais sensíveis de cada organização e eliminar riscos associados ao uso de um dispositivo próprio do funcionário ao administrar a informação da empresa.

Ao virtualizar seu ambiente de trabalho, é possível fazer com que o usuário faça suas atividades a partir uma localização remota em um ambiente onde é possível adicionar mais medidas de controle. Desse modo, tanto os aplicativos como a informação que se manipula, estarão sob o controle da empresa. Inclusive, os arquivos permanecem dentro dos servidores corporativos e em nenhum momento passam ao dispositivo desde que o usuário acessa.

Não é um método infalível, mas se é possível adicionar um nível a mais de proteção ao limitar que a informação seja processada diretamente no dispositivo do funcionário. Obviamente isso deve estar acompanhado dos controle apropriados para evitar possíveis fuga de dados.

Continuidade do negócio

Quando todos os funcionários se encontram em um mesmo escritório, a empresa costuma ter um plano para recuperar operações caso haja algum incidente. Do mesmo modo, é necessário contar com esse plano quando se implementa o trabalho a distância e os colaboradores estão fora da companhia.

Não obstante, ao contar com um esquema de trabalho remoto, ou seja, com equipamentos fora da infraestrutura comprometida, o processo de restauração se torna mais eficaz para garantir a continuidade do negócio; isso se deve porque somente é preciso focar esforços na infraestrutura mais crítica.

No mesmo contexto, é ideal contar com os sistemas virtuais, já que permitiria descentralizá-los em diferentes provedores e, assim reduzir o impacto de um possível incidente. Dessa maneira, caso ocorresse um incidente que afetaria a continuidade das operações - como uma falha elétrica nos escritórios ou um ataque que comprometeria o acesso à Internet -, aqueles que estão conectados por fora não vão se prejudicar e poderão seguir com suas atividades. Caso o incidente seja capaz de afetar o dispositivo físico de um funcionário, ele poderá utilizar outro para acessar ao ambiente virtualizado e continuar com suas atividades.

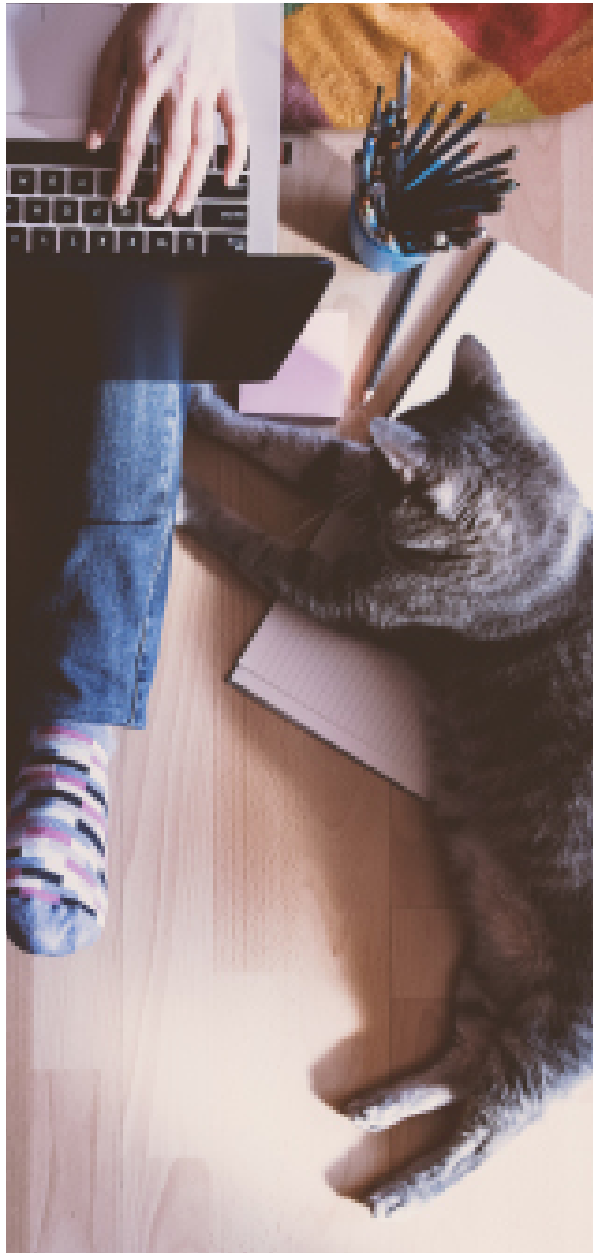
Além do contrato profissional

Se o funcionário manipula a informação da empresa em seu dispositivo pessoal, deve estar claro que ele terá que passar esses dados após o término de contrato, já que é difícil saber se a informação será eliminada.

Se bem a empresa pode oferecer os equipamentos para que o empregado realize seu trabalho, e dessa maneira recuperá-lo ao final de uma relação contratual, o risco de uma fuga de informação segue sendo bastante provável. Contar com os dados em depósitos administrados pela empresa e cuidar das permissões de acesso e modificação reduzem a possibilidade de uma fuga.

Do mesmo modo, outras ações de controle podem se apoiar em aspectos contratuais, como assinar acordos de confidencialidade ou medidas mais estritas com relação ao tipo de informação que podem ser baixadas e armazenadas em tais dispositivos.

É necessário falar previamente com o funcionário sobre a administração de informações da empresa, mesmo trabalhando com seu dispositivo pessoal ou um oferecido pela empresa.



7 pilares de segurança

1 GERENCIAR FUNÇÕES

É essencial certificar-se que o acesso à informação é permitido somente para as funções habilitadas para ela.

Para isso, é necessário estabelecer as responsabilidades na empresa de acordo com os objetivos de funcionários e também os envolvidos na gestão. Aspectos como o controle de tecnologias, realizações de backup, contar com processos de recuperação, entre outros, são algumas das tarefas que devem possuir um responsável e um momento definido.

Do mesmo modo, os funcionários relacionados ao trabalho a distância devem conhecer as políticas e, além disso, obter as permissões necessárias para realizar suas tarefas, já que deixar os perfis em modo padrão, sem controle ou sem políticas de acesso pode gerar problemas de segurança.

2 CONTROLE DE DISPOSITIVOS

Levando em consideração a ampla variedade de dispositivos no mercado, é importante restringir o acesso somente para aqueles que aplicam as ferramentas de segurança de forma adequada.

Nesse sentido, não é a mesma coisa se um funcionário acessar informações a partir de seu computador pessoal com um sistema operacional atualizado e com uma solução de segurança instalada, e se o faça partir de um tablet desatualizado, sem proteção e que várias pessoas utilizam para jogar e baixar aplicativos.

Portanto, é necessário considerar por qual dispositivo você irá permitir o acesso à informação corporativa.

3 PROTEGER CONTRA CÓDIGOS MALICIOSOS

Para garantir que nenhum código malicioso afete os dados, todos os dispositivos utilizados pelo empregado devem contar com soluções de segurança que sejam capazes de detectar de maneira proativa esse tipo de ameaças.

Se o dispositivo a partir do qual o funcionário utiliza não é da empresa, e além disso, não se utilizam ambientes virtuais, os riscos de sofrer uma infecção com códigos maliciosos são mais altos. A mesma condição se aplica para dispositivos móveis.

Além de uma solução de segurança, é necessário que o computador ou dispositivo móvel tenha todos os seus aplicativos atualizados. Portanto, a política de atualização deve ser clara para não dar lugar a vulnerabilidades.

4 MONITORAR O TRÁFEGO DE REDE

Dado que existem dispositivos que estão acessando a rede fora do perímetro físico do escritório, é necessário realizar um seguimento sobre o tipo de tráfego gerado. Por exemplo, por onde costumam acessar, se há muitas tentativas frequentes e falhas de acesso ao servidor, ou ainda, geram algum tipo de tráfego inapropriado, como o download de arquivos desconhecidos.

Outro aspecto importante, é a possibilidade de criar regras de tráfego que permitem verificar o comportamento da rede quando se realiza alguma mudança, seja a inclusão de alguma nova tecnologia ou serviço, fazendo com que seja possível determinar o uso e o que os usuários que estão fora da rede fazem.

5 CONEXÕES SEGURAS

Uma VPN (Virtual Private Network) é um tecnologia de rede que é utilizada para conectar um ou mais computadores a uma rede privada utilizando a Internet.

Ao implementar essa ferramenta, a empresa possui uma maior certeza de que quando seus funcionários quiserem acessar recursos corporativos a partir de suas casas, um hotel ou um restaurante, isso será realizado de forma segura.

Para esses casos de trabalho a distância, a implementação de conexões VPN baseadas no cliente é o mais apropriado, já que esse tipo de rede permite manter o usuário conectado a partir de uma rede remota, através de um aplicativo que se encarrega de estabelecer a comunicação com a VPN.

Para acessar a uma conexão segura, o usuário deve executar o aplicativo e se autenticar com um nome de usuário e senha, incluindo um segundo fator de autenticação. Desse modo, um canal criptografado é criado entre o equipamento e a rede remota, para uma troca segura de dados.

6 CRIAR UMA POLÍTICA DE SEGURANÇA

Na política de segurança é necessário declarar as intenções quanto a proteção dos recursos informáticos, e a partir dela estabelecer as bases para determinar as obrigações e responsabilidades dos usuários quanto ao uso das tecnologias que possuem a sua disposição.

Portanto, essa política deve definir que tipo de ações podem ser feitas e quem está habilitado para executá-las. Não é o mesmo tentar modificar uma base de dados por parte de um usuário que está fora da empresa, em vez de poder realizar consultas e informes.

Cada política é própria da realidade da organização e do alcance estabelecido para os empregadoas que fazem parte do trabalho a distância. Não obstante, é necessário reconhecer os ativos da informação, já que não se pode controlar aquilo que não se conhece seu estado.

7 CONSCIENTIZAR OS EMPREGADOS

A educação deve ser um pilar importante para que todos os usuários sejam conscientes dos riscos aos quais podem estar expostos e quais são os cuidados que devem ter ao acessar dispositivos que não são da companhia.

Se o usuário não conhece os riscos aos quais expõe a informação da empresa, e incluindo seus próprios dados, pode se tornar vítima de muitas ameaças com mais facilidade. O funcionário deve entender que assim que estiver fora do escritório, o dispositivo que utiliza para trabalhar é uma porta de qualquer organização e é necessário garantir seu uso adequado.

Evolução e melhora contínua

A melhora contínua é um conceito que vem dos sistemas de gestão, e que para casos de implementações importantes, como a do trabalho a distância, é crucial para um bom funcionamento. Portanto, é necessário avaliar e medir a forma com que as atividades daqueles que trabalham de forma remota vão se desenvolvendo, sempre levando em consideração a política e os objetivos de segurança e informar os resultados.

É a partir dessa informação que se pode implementar as mudanças necessárias para melhorar os processos. Para que essas atividades obtenham êxito, deve-se monitorar o uso dos ativos da informação para detectar mudanças nos possíveis riscos que podem surgir.

Por exemplo, cada vez que se realiza uma mundança na infraestrutura mais crítica ou quando alguma política de segurança muda, é importante verificar se todos realizam suas atividades de acordo com tais mudanças. O surgimento de uma nova vulnerabilidade ou atualização de alguma das ferramentas utilizadas para se conectar de forma remota podem ser utilizadas por invasores para chegar à informação sensível.

Não basta implementar um programa de trabalho a distância de forma exemplar, a chave para que realmente seja possível aproveitar e gerar os benefícios esperados é que se faça um acompanhamento de como ela foi implementada.

Conclusão

A adoção de uma metodologia de trabalho a distância pode trazer grandes benefícios relacionados a diminuição de gastos na infraestrutura, a comodidade dos funcionários para a administração da informação e, portanto, um aumento de produtividade; não obstante, a empresa enfrenta novas ameaças que devem ser gerenciadas. Estamos tratando principalmente de fuga de dados e acessos não autorizados à informação. Para enfrentar esses desafios, as organizações devem realizar uma combinação entre políticas clara para o gerenciamento da informação e o uso de ferramentas adequadas que permitem sua gestão de segurança. Do mesmo modo, não se pode deixar de lado a educação dos empregados para que conheçam os riscos e saibam como pode enfrentá-los.

O acesso à informação corporativa por parte de pessoas alheias à empresa e consequentemente a fuga dos daos, muitas vezes, pode deixar sequelas econômicas para recuperar ou reparar os danos causados. Nesse sentido, barreiras de prevenção como programas de criptografia, senhas e firewall contra ataques a partir da rede podem evitar mais de uma simples dor de cabeça.

O trabalho a distância não é uma opção viável para todas as empresas, e ainda se uma companhia decide realizar essa metodologia, talvez não será aplicada para todas as áreas. Para mudar a forma de trabalhar em uma organização, é importante realizar um bom planejamento e que a implantação seja progressiva, avaliando os resultados obtidos.

A melhora contínua do processo, a implementação de controles de segurança e a conscientização dos funcionários será fundamental para que se possa obter um ambiente de trabalho seguro. Dessa maneira, a organização poderá contar com um ambiente suficientemente robusto conhecendo o tipo de dispositivos que podem se conectar, e com métodos de acesso seguros e definidos, independentemente do foco (físico ou virtual) que se escolheu.

Depois de tudo, para poder estar alinhado com os avanços da tecnologia é necessário se concentrar na gestão de segurança da informação, mais que na segurança da infraestrutura, e o trabalho a distância é um grande exemplo dessas práticas.

www.eset.com/br

/EsetBrasil @ESET_Brasil /company/eset-brasil