ORIENTAÇÕES GERAIS PARA TRABALHO REMOTO (*HOME OFFICE*)

Sob a ótica da privacidade e segurança da informação

1. PARA OS COLABORADORES QUE TRABALHAM EM AMBIENTE VIRTUAL DE FORMA REMOTA:

- Se possível utilizar dispositivo corporativo e não o utilizar para uso pessoal;
- Evitar e se possível fechar portas para utilização de *pendrives, hd´s* externos e outros periféricos;
- Nunca acesse uma rede *Wi-Fi* pública para realizar suas atividades do trabalho (ex: shoppings, aeroportos, restaurantes);
- Nunca envie ou abra documentos confidenciais quando estiver conectado ao *Wi-Fi* público ou *Bluetooth* não seguros;
- Sempre desligue *Wi-Fi* e Bluetooth do seu dispositivo quando não estiverem em uso;
- Sempre se conecte a uma rede virtual privada (VPN) para que o tráfego da Internet seja criptografado, principalmente se estiver conectado a uma rede *Wi-Fi* pública;
- Se a sua empresa não possuir VPN, procure utilizar drives de mercado, tais como *OneDrive, Dropbox, Gsuite*, dentre outros;
- Não utilize o mesmo login e senhas do trabalho para acessos particulares;
- Se possível a área responsável deverá estabelecer políticas de senhas seguras, com renovações por períodos mais curtos;
- Nunca marque a caixa de seleção "Lembrar-me" ao acessar seus e-mails, armazenamento e outros aplicativos em nuvem on-line;
- Salve documentos e arquivos em nuvem, ao invés de mantê-los em seu dispositivo;
- Nunca use dispositivos, como celulares e notebooks pessoais, para armazenar dados confidenciais, a não ser que sejam criptografados;

- Verifique se dispositivo utilizado possui softwares e ferramentas de segurança atualizados, como aplicativos, antivírus, firewalls, software de filtragem da web e criptografia de dispositivo;
- Utilizar, sempre que possível, filtros de privacidade de tela do dispositivo para evitar olhares invasivos de pessoas próximas do dispositivo;
- Estabeleça filtros de acesso mais restritivos a sites e redes sociais;
- Estabeleça a autenticação de dois fatores, principalmente em aplicativos online e de mensageria.
- Orientar colaboradores sobre impressão de documentos e forma de descarte de papéis e informações impressas;
- Implementar registros de auditoria sobre acesso e utilização de informações pessoais nos bancos de dados e sistemas da empresa;
- Se possível, e não for prejudicial ao desenvolvimento da atividade empresarial, limitar os horários de acesso, quando não houver monitoramento permanente;

2. CAUTELAS QUANTO ÀS INFORMAÇÕES E DADOS CONTIDOS EM AMBIENTES FÍSICOS:

A preocupação deve abranger não apenas o ambiente virtual, mas também os ambientes físicos, sugerindo-se:

- Que sejam estabelecidas regras de controle de acesso aos locais onde são armazenados documentos e informações físicas;
- Se houver necessidade de deslocamento do documento físico para fora da empresa, que seja estabelecido registro e rastreabilidade desses documentos e informações;
- Orientar os colaboradores com informações suficientes sobre como transportar, manusear, armazenar referidos documentos e informações, bem como sobre como e em que prazo os restituir à empresa;

As orientações aqui tratadas representam um mínimo de boas práticas no desenvolvimento do trabalho remoto e não têm a pretensão de esgotar o tema, tampouco afasta a necessidade

de uma análise caso a caso, por cada uma das diversas áreas multidisciplinares da sua corporação que tratam dados pessoais, conectadas com o programa de privacidade e políticas estabelecidas.

Para outras contribuições e esclarecimentos, contate-nos:

Março de 2020

SEUSDADOS CONSULTORIA EM GESTÃO DE DADOS LTDA.

www.seusdados.com

+55 11 4587 2900

laura@seusdados.com

marcelo@seusdados.com

in/seusdados

in/marcelofattori