Sumário

1. OBJETIVO 2
2. ELEGIBILIDADE PARA O TRABALHO EXTERNO 3
3. DIRETRIZES GERAIS 4
4. RESPONSABILIDADES 5

1. Objetivo

O objetivo principal desse procedimento é estabelecer um processo controlado e seguro para habilitar o acesso remoto (VPN) aos colaboradores que estão realizando trabalhos externos. O procedimento visa garantir a segurança da rede, proteger os dados da organização e assegurar o cumprimento da jornada de trabalho, enquanto permite a flexibilidade necessária para que os colaboradores executem suas atividades fora do escritório.

Objetivos específicos incluem:

Segurança da Informação:

- Assegurar que o acesso remoto seja concedido de maneira segura, com medidas de autenticação e criptografia adequadas para proteger os dados sensíveis da organização.

Controle e Autorização:

- Estabelecer um processo formalizado que exige a aprovação do diretor responsável antes de conceder acesso remoto, garantindo que a liberação seja justificada e alinhada aos objetivos da organização.

Cumprimento da Jornada de Trabalho:

- Garantir que os colaboradores em trabalho externo respeitem a jornada de trabalho estabelecida, evitando o uso indevido do acesso remoto para atividades pessoais.

Rastreabilidade e Auditoria:

- Possibilitar a realização de auditorias periódicas para monitorar o uso adequado do acesso remoto, identificar potenciais irregularidades e garantir a conformidade com as políticas da empresa.

Eficiência Operacional:

- Facilitar a continuidade operacional ao permitir que os colaboradores acessem os recursos necessários de forma remota, contribuindo para a produtividade mesmo em situações em que o trabalho presencial não seja viável.

Suporte Técnico Efetivo:

- Garantir que os colaboradores tenham acesso a suporte técnico quando necessário, minimizando interrupções nas atividades e promovendo uma experiência positiva de uso da VPN.

Adaptação à Mobilidade:

- Capacitar a força de trabalho para realizar tarefas de forma eficaz fora do escritório, apoiando iniciativas de trabalho remoto ou mobilidade corporativa.

2. Elegibilidade para o trabalho externo

São elegíveis ao trabalho externo todos os colaboradores da **ITAESBRA**, desde que:

I. Não precisem, necessariamente, estar no escritório para trabalhos que exijam sua presença;
II. Não possuam reuniões agendadas com clientes, sobre assuntos considerados estritamente confidenciais, para o caso ou para o escritório; ou que o cliente não possa ou não aceite que elas ocorram remotamente.
III. Os gestores das áreas terão o acesso liberado a VPN e sem restrição de horário.

3. Diretrizes Gerais

I. Solicitação:

- O gestor responsável pelo colaborador externo deve enviar uma solicitação à equipe de Tecnologia de Informação (T.I) com 48 horas de antecedência.
- A solicitação deve ser encaminhada por e-mail, com o diretor responsável pela área em cópia.
- A solicitação deve conter as seguintes informações:
- Motivo da liberação do acesso remoto.
- Data e horário específicos para habilitação do acesso.

II. Aprovação:

- A solicitação será submetida ao diretor responsável para aprovação.
- A aprovação deve ser registrada por e-mail.

III. Configuração do Acesso Remoto:

- Após a aprovação, a equipe de T.I. procederá com a configuração do acesso remoto para o colaborador em questão.
- Será fornecida ao colaborador a informação necessária para a acesso da VPN em seu notebook.

IV. Utilização Responsável:

- Os colaboradores devem utilizar o acesso remoto de forma responsável, respeitando a jornada de trabalho.
- O acesso remoto destina-se apenas a atividades relacionadas ao trabalho, e qualquer uso indevido será sujeito a medidas disciplinares.

V. Encerramento do Acesso:

- O acesso remoto será encerrado automaticamente no término do horário autorizado.
- Caso seja necessário estender o acesso, uma nova solicitação deverá ser feita com antecedência.

VI. Auditoria:

- A equipe de T.I. realizará auditorias periódicas para garantir o uso apropriado do acesso remoto.

VII. Suporte Técnico:

- Em caso de problemas técnicos, os colaboradores podem contatar a equipe de suporte técnico de T.I.

VIII. Uso Consciente:

- Use uma conexão VPN (Rede Privada Virtual) para criptografar sua conexão com a internet e proteger os dados que estão sendo transmitidos.
- Evite o uso de redes Wi-Fi públicas e não seguras (sem senhas). Se for necessário usá-las, evite a transmissão de informações confidenciais.
- Não compartilhe senhas com ninguém durante o trabalho externo.
- Utilize senhas para bloquear seu dispositivo sempre que não estiver sendo usado. Isso impede o acesso não autorizado em caso de ausência temporária, perda ou roubo.
- Limite o acesso a informações sensíveis quando estiver em áreas movimentadas. Evite armazenar dados confidenciais em dispositivos móveis, a menos que seja estritamente necessário.
- Esteja atento a pessoas que possam tentar observar o que você está fazendo em seu dispositivo, em especial em áreas movimentadas, como: aeroportos, rodoviárias, cafés, restaurantes, etc... Ajuste o brilho da tela para reduzir a visibilidade.
- Limpe a tela do seu notebook de informações confidenciais assim que não forem mais necessárias.

4. Responsabilidades

Compete à área de Tecnologia da Informação (TI):

I. Implementar e manter a norma de trabalho externo, regularmente revisada, considerando os requisitos legais e do negócio, assegurando a adequada formalização e comunicação para as partes interessadas.
II. Implementar a gestão operacional das tecnologias que garantam a segurança dos acessos externos ao ambiente da **ITAESBRA**.
III. Configurar e garantir que todas as configurações e proteções de segurança (antivírus, firewall, criptografia, vpn, etc.) sejam instaladas nos dispositivos móveis.
IV. Apagar com segurança, o conteúdo do disco local dos dispositivos móveis, antes que o dispositivo seja realocado para outra finalidade ou descartado.
V. Garantir os controles e as medidas de proteção física para segurança dos dispositivos.

Compete à área de SI (Segurança da Informação) :

I. Observar e zelar pelo cumprimento da presente Norma e, quando assim se fizer necessário, acionar a Diretoria para consulta sobre situações que envolvam conflito com esta Norma ou mediante a ocorrência de situações nela descritas.
II. Controlar e monitorar qualquer tipo de acesso externo fornecido pela **ITAESBRA**.
III. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso externo e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

Compete à Diretoria e Gerência:

I. Aprovar a concessão ou revogação do uso de dispositivos móveis de colaboradores e terceiros aos sistemas da companhia.
II. Aprovar a concessão ou revogação do acesso externo dos colaboradores e terceiros sob sua gestão.

Compete aos Funcionários, Estagiários e Terceiros:

I. Devem estar cientes de suas responsabilidades às regras de trabalho externo estabelecidas nesta norma.

Esta norma deve ser revisada anualmente ou quando for necessária a alteração.

Controle de Revisão do Documento				
Nº	**Data**	**Elaborado por**	**Histórico da Revisão**	**Revisado por**
00	13/11/23	Julio Nicolosi	Publicação inicial	Janduir Tavares