



Boas Práticas

Criptografia de Disco
N-able N-sight RMM

Aviso legal

As informações e o conteúdo deste documento são fornecidos apenas para fins informativos e são fornecidos "no estado em que se encontram", sem garantia de qualquer tipo, expressa ou implícita, incluindo, mas não se limitando às garantias implícitas de comercialização, adequação a um fim específico, e não violação. A ADDEE não se responsabiliza por quaisquer danos, incluindo danos consequenciais, de qualquer tipo que possam resultar do uso deste documento e das ferramentas nele citadas. As informações do presente documento são obtidas de fontes publicamente disponíveis.

Sumário

Introdução	3
1. Pré-Requisitos	4
+ Sistemas Operacionais	4
+ BitLocker	4
2. Ativar (Política MAV-BD)	5
+ Considerações	6
3. Formas de Ativação	7
+ INDIVIDUAL (por dispositivo)	7
+ MASSIVA (por cliente/site)	8
+ Considerações	9
4. Instalação	10
+ Considerações	11
5. Monitorar	12
6. Relatórios	13
+ Considerações	14
7. Chave de Recuperação (usuário final)	15
+ Considerações	15
8. FAQ	16
9. Obrigado!	17

Introdução

A criptografia de disco tem como objetivo proteger os dados de seus clientes num eventual roubo ou perda acidental, tornando as informações em discos rígidos ilegíveis para usuários não autorizados.

Ela é ideal quando os dados são um ativo crítico ou regidos por regulamentações de conformidade, como **LGPD, GDPR, PII, PCI DSS**, e também quando há risco de perda de dados.

Usando a criptografia de disco, os dados não podem ser acessados e as informações não podem ser roubadas. As chaves de criptografia estão conectadas ao hardware no qual o disco está instalado para garantir que a simples remoção de um disco não forneça acesso aos dados.

Mesmo se a unidade de disco for removida do computador, as informações permanecerão criptografadas e não poderão ser recuperadas sem as **Chaves de Recuperação** associadas.

A segurança oferecida pela criptografia de disco proporciona tranquilidade, principalmente quando ativada nos dispositivos de risco, como por exemplo em laptops, que normalmente são usados também fora do escritório.

A criptografia de disco é integrada ao MAV-BD (Managed Antivírus Bitdefender) e implantada pelas políticas de proteção do MAV-BD, portanto para que você possa utilizar este módulo é necessário que o dispositivo tenha o recurso do MAV ativado e com a Criptografia de Disco habilitada.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para boaspraticas@addee.com.br.

1. Pré-Requisitos

+ Sistemas Operacionais

Através [deste link](#) você tem acesso a página do manual do recurso, onde descreve todas as versões do sistema operacional Windows, compatíveis com a Criptografia de Disco.

+ BitLocker

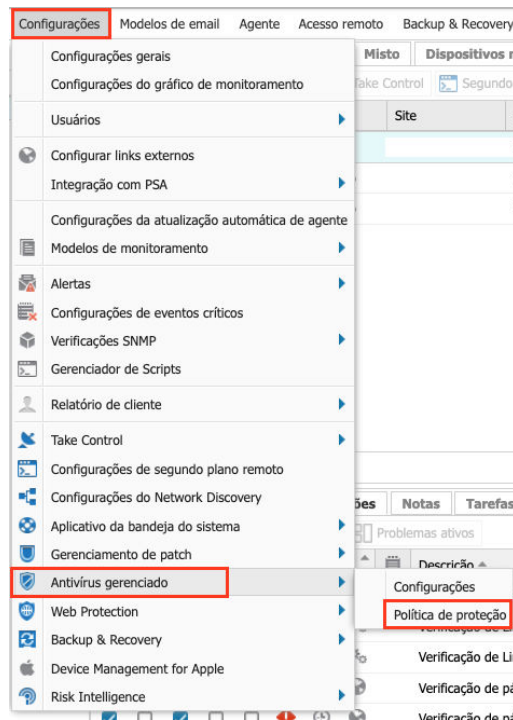
Os sistemas operacionais que são suportados e listados nos pré-requisitos acima devem ter o **BitLocker** instalado/ativado para que o Gerenciador de Criptografia de Disco gerencie a criptografia de disco.

Se o BitLocker não estiver disponível, o Gerenciador de Criptografia de Disco não será instalado e na guia Resumo do dispositivo mostrará que o BitLocker está ausente, junto com a mensagem de “Não Suportado”.

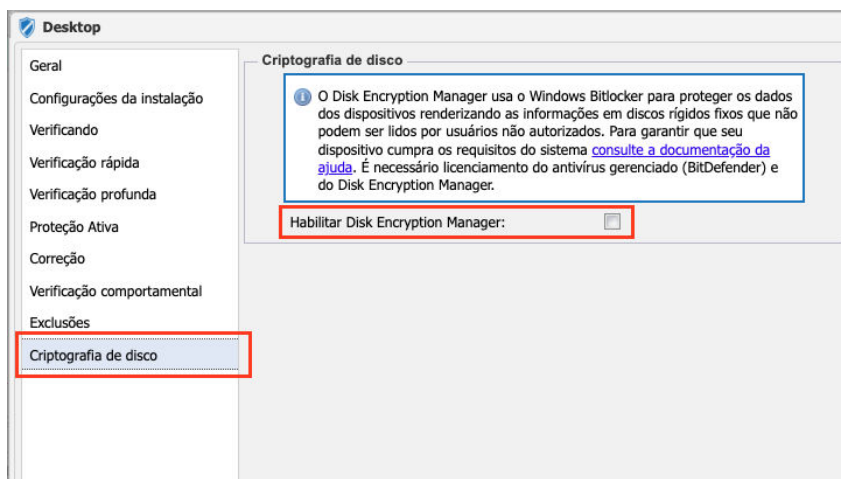
2. Ativar (Política MAV-BD)

O **Disk Encryption Manager** é ativado ou desativado através da política de proteção do MAV-BD.

Para isto, acesse o menu *Configurações / Antivírus Gerenciado / Política de Proteção*.



Após escolher e editar a política a ser utilizada localize o menu Criptografia de Disco, do lado esquerdo da janela, e marque a check box para ativar o recurso (ou desmarque-a para desativá-la).



Observação: Lembre-se que aqui você está apenas ativando a Criptografia de Disco na política do MAV-BD. No passo "4. Instalação" explicaremos como ativar a Criptografia de Disco no dispositivo, que é necessária para o funcionamento do recurso.

+ Considerações

- Onde a política de proteção do MAV-BD foi definida no nível do dispositivo individual, mover o dispositivo para outro Cliente ou Site não alterará a política de proteção.
- Dependendo das alterações nos requisitos e nas necessidades de proteção do seu cliente, talvez você precise aplicar uma nova política de proteção do MAV-BD a seus dispositivos, ou até mesmo mover os dispositivos entre Clientes e/ou Sites.
- Deve-se tomar cuidado ao executar estas ações, pois os dispositivos com políticas herdadas do nível do Site ou do Cliente serão atualizados para corresponder à configuração do Gerenciador de Criptografia de Disco do MAV-BD, conforme definido nas configurações da nova política. A política não será alterada quando definida no nível do dispositivo individual.
- Quando você move dispositivos ou troca a política de proteção de onde o Disk Encryption Manager está desativado para onde está ativado, todos os dispositivos instalam o Disk Encryption Manager e criptografam o dispositivo.
- Quando você move dispositivos ou troca a política de proteção de onde o Disk Encryption Manager está ativado para onde está desativado, todos os dispositivos desinstalam o Disk Encryption Manager e descriptografam os dispositivos.

3. Formas de Ativação

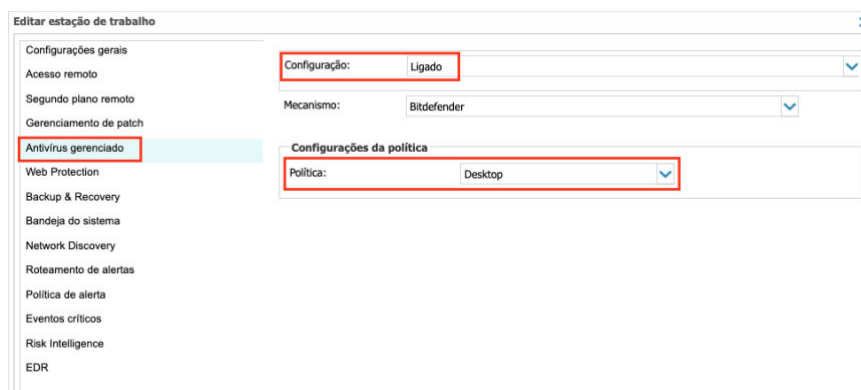
Como o Disk Encryption Manager é um módulo do MAV-BD, o MAV-BD deve estar instalado no dispositivo. A ativação do Disk Encryption Manager é realizada nas definições de configuração da política de proteção do MAV-BD.

Assim, para ativar ou desativar o Gerenciador de Criptografia de Disco por tipo de dispositivo, cliente ou site, uma política de proteção MAV-BD adequada deve ser usada conforme mencionado no item **“2. Ativar (Política MAV-BD)”**.

É possível ativar o recurso de duas formas:

+ INDIVIDUAL (por dispositivo)

Você pode ativar o recurso de forma individual, dispositivo por dispositivo, editando o dispositivo em questão, acessando o menu Antivírus Gerenciado e, após ativar o recurso, vincular uma política que esteja com a Criptografia de Disco ativada.



Caso você não tenha uma política com este recurso ativado você deverá editar ou criar uma nova política e ativar o recurso. No passo anterior é explicado como realizar este procedimento.

Observação: A instalação do Disk Encryption Manager não requer a reinicialização do dispositivo.

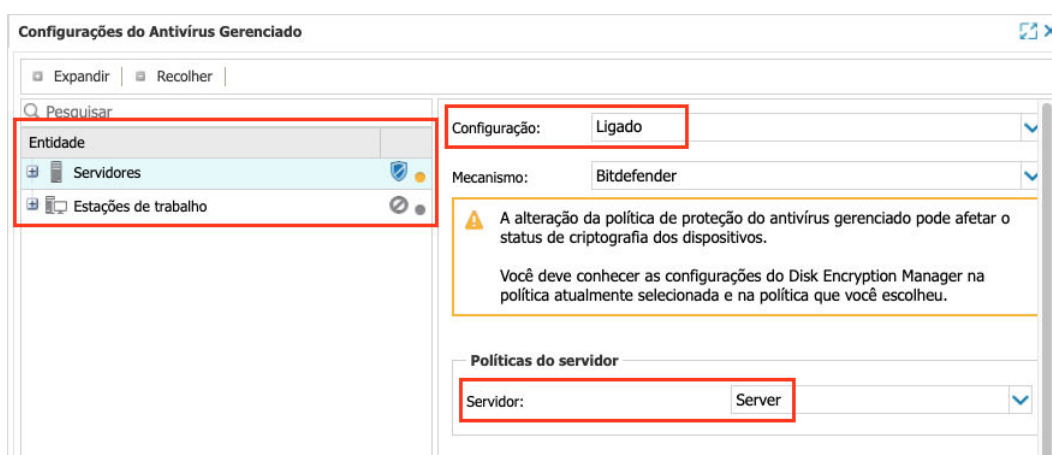
Se houver dispositivos com unidades já criptografadas com BitLocker, quando o MAV-BD executar a instalação do Disk Encryption, o sistema não precisará criptografar novamente. A capacidade de gerenciamento será assumida pelo N-

sight RMM, e as chaves de recuperação geradas serão armazenadas no próprio N-sight RMM. **O usuário final não verá nenhum impacto no seu dispositivo.**

+ **MASSIVA (por cliente/site)**

Caso queira ativar o recurso de forma massiva, seja para um cliente ou um site, você pode realizar da seguinte maneira:

- Acesse o menu *Configurações / Antivírus Gerenciado / Configurações*.
- Escolha a entidade que terá o recurso ativado (todos os clientes ou um cliente/site específico, seja Servidores ou Estações de Trabalho), ative o recurso e escolha uma política que possui o Disk Encryption ativado.



Caso você não tenha uma política com este recurso ativado você deverá editar ou criar uma nova política e ativar o recurso. No passo anterior é explicado como realizar este procedimento.

Observação: A instalação do Disk Encryption Manager não requer a reinicialização do dispositivo.

Se houver dispositivos com unidades já criptografadas com BitLocker, quando o MAV-BD executar a instalação do Disk Encryption, o sistema não precisará criptografar novamente.

A capacidade de gerenciamento será assumida pelo N-sight RMM, e as chaves de recuperação geradas serão armazenadas no próprio N-sight RMM.

O usuário final não verá nenhum impacto no seu dispositivo.

+ Considerações

- As implantações do Disk Encryption Manager são configuradas e iniciadas no RMM. Dependendo da configuração do computador e/ou seleção de política, será solicitado ao usuário do dispositivo inserir um PIN ou senha como parte do processo de instalação e após a instalação quando o computador iniciar.
- A criptografia de um disco pode levar algum tempo para ser concluída, aproximadamente um minuto para cada 500 MB. O tempo gasto depende dos recursos do dispositivo e se está em uso no momento.
- Se o usuário desligar o computador durante o processo de criptografia, a criptografia será retomada assim que o dispositivo voltar a funcionar.
- O Gerenciador de Criptografia de Disco não oferece suporte ao “BitLocker to Go” para dispositivo de armazenamento removíveis.

4. Instalação

Durante a instalação do Disk Encryption Manager, o usuário encontrará três cenários:

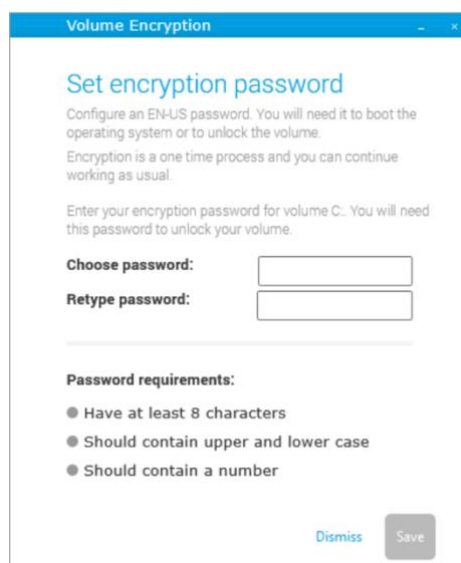
1 – Se o dispositivo **não tiver TPM (Trusted Platform Module)**, o usuário será solicitado a definir uma senha de criptografia usada para desbloquear o disco para usar o computador.

A senha deve ter oito caracteres e incluir pelo menos uma letra maiúscula, uma minúscula e um número. O usuário pode ignorar a solicitação.

Se um usuário não digitar a senha necessária, ele receberá um aviso a cada poucos minutos, lembrando-o de concluir a instalação.

2 – Se o dispositivo **tiver TPM (Trusted Platform Module)**, e **you selecionou solicitar um PIN ao usuário**, ele deverá definir um PIN. O PIN de criptografia deve ter entre seis e 21 caracteres alfanuméricos.

3 – Se o dispositivo **tiver TPM (Trusted Platform Module)** e **you não selecionou a opção de PIN digitado pelo usuário**, nenhuma interação será necessária.



The screenshot shows a window titled "Volume Encryption" with a blue header. The main content area is titled "Set encryption password" in blue. Below the title, there is explanatory text: "Configure an EN-US password. You will need it to boot the operating system or to unlock the volume. Encryption is a one time process and you can continue working as usual." This is followed by another instruction: "Enter your encryption password for volume C:. You will need this password to unlock your volume." There are two input fields: "Choose password:" and "Retype password:". Below these fields, a section titled "Password requirements:" lists three bullet points: "Have at least 8 characters", "Should contain upper and lower case", and "Should contain a number". At the bottom right, there are two buttons: "Dismiss" and "Save".

Após esta etapa, o Disk Encryption Manager primeiro criptografa a unidade de inicialização e continua com as unidades adicionais.

Não há opção para criptografar apenas as unidades selecionadas.


Uma mensagem é exibida informando ao usuário quando o processo de criptografia começa incluindo a unidade e a hora de início. Outra mensagem é exibida para o usuário final quando o processo de criptografia é concluído.

No [manual](#) você encontra mais detalhes sobre isto.

+ Considerações

- Caso um usuário final remova o BitLocker do sistema por meio do painel de controle (Adicionar ou Remover Programas) quando o dispositivo for criptografado com o Disk Encryption Manager, a verificação do serviço de criptografia de disco (Bitdefender) apontará uma falha. O usuário final será obrigado a reinstalar o BitLocker para resolver a falha.
- A instalação do Disk Encryption Manager não requer uma reinicialização do dispositivo.
- Se houver dispositivos com unidades já criptografadas com BitLocker, quando o MAV-BD executar a instalação do Disk Encryption, o sistema não precisará criptografar novamente. A capacidade de gerenciamento será assumida pelo N-sight RMM, e as chaves de recuperação geradas serão armazenadas no próprio N-sight RMM. **O usuário final não verá nenhum impacto no seu dispositivo.**

5. Monitorar

Uma nova coluna é adicionada ao painel Norte quando o Gerenciador de Criptografia de disco estiver ativado em pelo menos um dispositivo ().

Esta coluna (como as outras) pode ser arrastada para uma posição mais adequada para a visualização, se necessário.










Após ativar a Criptografia de Disco, duas verificações de monitoramento são adicionadas automaticamente ao dispositivo, para o monitorar o status do Disk Encryption Manager. São elas:

+ Verificação de serviço do Gerenciador de Criptografia de Disco (Bitdefender)

Esta verificação monitora o serviço do Gerenciador de Criptografia de Disco. A verificação passa quando o serviço é relatado como em execução e falha quando o serviço está em qualquer outro estado.

+ Verificação do Gerenciador de Criptografia de Disco (Bitdefender) - <letra da unidade de disco>

O RMM adiciona automaticamente esta verificação para cada unidade no dispositivo.

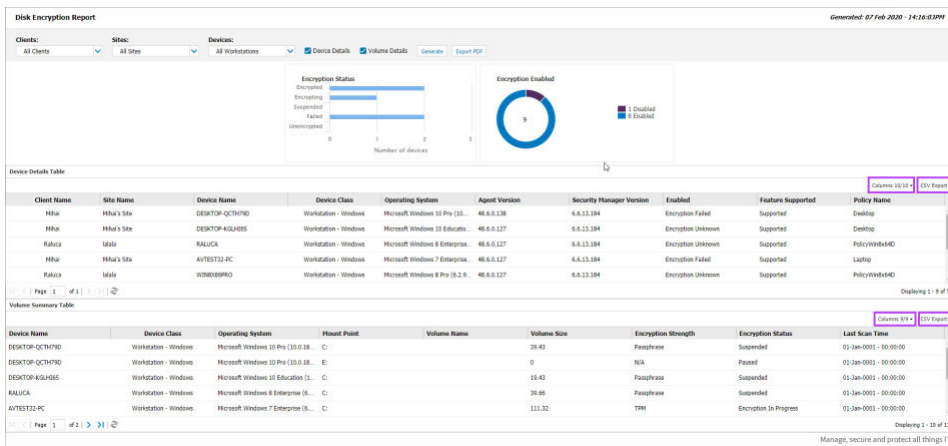
Summary	Outages	Checks	Notes	Tasks	Assets	Antivirus
+ Add Check ▾ Check ▾						
					Description	More Information
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 Disk Encryption Manager Check (Bitdefender) - C:	Encrypted
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 Disk Encryption Manager Service Check (Bitdefender)	Encrypted
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 Managed Antivirus Check (Bitdefender)	More information
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 Managed Antivirus Update Check (Bitdefender)	53870

Mais detalhes das verificações acima você encontra [neste link](#).

6. Relatórios

Existem 2 relatórios dedicados disponíveis no N-sight RMM para o Gerenciamento de Criptografia de Disco. São eles:

1. **Relatório de Criptografia de Disco:** Este relatório fornece uma visão geral gráfica dos status de criptografia e da criptografia ativada x desativada por padrão.



2. **Relatório da Chave de Recuperação:** Este relatório fornece uma lista de TODAS as chaves de recuperação e o ID da chave / ID do protetor / ID da chave de recuperação associado em um único local.

Mais detalhes dos relatórios acima você encontra [neste link](#).

+ Considerações

- Como o **Relatório da Chave de Recuperação** contém informações confidenciais e permite a descryptografia de todos os dispositivos listados, deve-se tomar cuidado ao atribuir permissões aos técnicos para acessar e executar este relatório.
- Se você encerrar a sua conta no N-sight RMM (de testes ou completa), precisará confiar no seu Relatório da Chave de Recuperação. Verifique se você produziu o relatório e o salvou com segurança para uso futuro antes de encerrar sua conta no N-sight RMM, pois não armazenamos nada no sistema, neste caso.
- **Se você excluiu seus dispositivos do N-sight RMM, a última chave de recuperação conhecida será mantida no relatório de chaves de recuperação por até 90 dias.**
- Se você remover o Gerenciador de Criptografia de Disco dos dispositivos, e eles permanecerem no N-sight RMM, você ainda terá acesso ao Relatório da Chave de Recuperação, que possui o histórico da última Chave de Recuperação conhecida antes que o dispositivo retorne o controle ao usuário final. Esteja ciente de que o usuário final pode ter criptografado novamente, o que alteraria a Chave de Recuperação do que o N-sight RMM possuía pela última vez registrado.
- **Nesses cenários, é altamente recomendável executar o Relatório da Chave de Recuperação e armazená-lo em um local seguro antes de executar outras ações. Caso contrário, você não poderá acessar as Chaves de Recuperação no N-sight RMM ou no suporte técnico.**
- Às vezes, você verá várias entradas para o mesmo dispositivo neste relatório, isto ocorre devido aos processos internos do BitLocker que atualizam as chaves de criptografia de um dispositivo (por exemplo, no caso de a unidade ter sido criptografada pelo BitLocker antes da implementação da Criptografia de Disco Gerente). Assim, quando um usuário precisar da Chave de Recuperação, a ID do Protetor oferecida pelo BitLocker durante a inicialização será uma das já utilizadas para a criptografia de disco nestes dispositivos. Para ajudar nisto, o relatório lista todos os Ids de Protetor e Chaves de Recuperação associados ao dispositivo.

7. Chave de Recuperação (usuário final)

As chaves de recuperação permitem que um usuário acesse o dispositivo criptografado se esquecerem sua senha ou se uma unidade criptografada precisar ser instalada em um novo computador.

[Neste link](#) do manual explicamos de forma detalhada como fazer esta restauração.

+ Considerações

Os dispositivos que usam o TPM sem uma opção de PIN não precisam digitar uma senha de pré-inicialização, mas exigirão as Chaves de Recuperação se a unidade de disco for movida para um novo dispositivo.

8. FAQ

1. Posso cancelar uma criptografia enquanto ela estiver em andamento?

Não há como cancelar o processo de criptografia. Uma solução alternativa é descriptografar o volume, desde que muito menos de 50% já esteja criptografado. Observe que a descriptografia é um processo intensivo de recursos.

2. Qual é a sequência de criptografia quando existem vários discos?

A criptografia começa com o disco de inicialização e, uma vez concluído, o Disk Encryption Manager continua com os restantes dos discos fixos. Não há capacidade de selecionar quais unidades criptografar e deixar outras não criptografadas. Todas as unidades fixas serão criptografadas.

3. Se eu adicionar uma nova unidade a um dispositivo, ela será criptografada se as outras unidades já estiverem criptografadas?

Sim. O Gerenciador de Criptografia de Disco verifica o dispositivo regularmente, ele detecta a nova unidade e inicia o processo de criptografia para a nova unidade.

4. Se acidentalmente enviar um documento por e-mail de um volume criptografado para um terceiro, será ilegível pelo destinatário?

Não. A criptografia está no nível do volume, não no nível do arquivo.

5. O Disk Encryption Manager criptografará uma unidade removível?

As unidades removíveis são ignoradas pelo Disk Encryption Manager e não são criptografadas.

Veja todas as FAQ's no nosso manual, através [deste link](#).

Obrigado!

Ficamos felizes por você utilizar este manual :)



Responsável: Caio Gutierri

Departamento: Engenharia de Vendas

Última alteração: Maio/2023

0800 761 2812

boaspraticas@addee.com.br