	<b>INSTRUÇÃO DE OPERAÇÃO</b>		<b>ITO-269</b>
	Título:		Revisão: <b>B</b>
	<b>USO DE DISPOSITIVOS USB E ARMAZENAMENTO REMOVÍVEL</b>		Página: <b>1 de 2</b>
	Departamento: <b>T.I</b>		Data de efetivação: <b>11/02/25</b>
Elaborador	Revisor	Aprovador	
Vitor Faustino	André Munerato	Carina Affonso	

## 1. OBJETIVO

O objetivo desta instrução é definir diretrizes detalhadas para o uso responsável de dispositivos USB e outros dispositivos de armazenamento removível por todos os funcionários, contratantes e terceiros com acesso a dados protegidos ou confidenciais da ORGANIZAÇÃO.

## 2. REFERÊNCIAS

- NBR ISO/IEC 27001
- NBR ISO/IEC 27002
- NBR ISO/IEC 27005
- ITO-259 Classificação da informação
- ITO-265 Utilização do Ambiente Internet pelo Usuário

## 3. ABRANGÊNCIA

Esta política se aplica a todos os dispositivos USB, incluindo unidades flash USB, discos rígidos externos, cartões de memória e quaisquer outros dispositivos de armazenamento removível, bem como a todos os funcionários, contratantes, consultores e terceiros que tenham acesso a informações confidenciais ou protegidas pela ORGANIZAÇÃO.

## 4. RESPONSABILIDADES

**Área de segurança da informação:** Garantir que os requisitos de segurança da informação sejam considerados quando do desenvolvimento, implantação e uso de sistemas de informação.

A área de segurança da informação coordenará as áreas técnicas, as áreas de apoio e as áreas de negócio para desenvolvimento e implantação de projetos, procedimentos, ações, instruções e normativos que possibilitem a operacionalização e manutenção desta política.

**Desenvolvedores de sistemas de informação:** Garantir que os requisitos de segurança da informação estejam implementados nos sistemas de informação que desenvolverem e mantiverem.

**Usuário:** Seguir as regras de segurança da informação.

**Chefias:** Garantir que os usuários tenham conhecimento e cumpram os requisitos de segurança da informação.

## 5. AUTORIDADE

O superior imediato tem autoridade definida para assegurar o cumprimento das normas de segurança, das instruções de operação e das normas e legislação em geral.

## 6. DEFINIÇÕES

**Dispositivo USB:** Qualquer dispositivo de armazenamento removível conectado por meio de uma porta USB.

**Usuário:** Agentes externos ao sistema ou pessoas que se utilizam dos recursos, serviços e/ou estruturas de tecnologia.


**Gestor da Informação (GI):** Cada informação deverá ter seu Gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação. O Gestor da Informação é o responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

## 7. EPI

N/A

## 8. DESCRIÇÃO DA ATIVIDADE

Todos os funcionários e partes interessadas devem solicitar autorização prévia do departamento de TI antes de conectar qualquer dispositivo USB aos sistemas ou redes da ORGANIZAÇÃO.

	<b>INSTRUÇÃO DE OPERAÇÃO</b>	<b>ITO-269</b>
	Título:	Revisão: <b>B</b>
	<b>USO DE DISPOSITIVOS USB E ARMAZENAMENTO REMOVÍVEL</b>	Página: <b>2 de 2</b>

#### 8.1. Tipos de Dispositivos USB Permitidos

- Apenas dispositivos USB aprovados pelo departamento de TI podem ser usados para armazenar ou transferir dados da empresa.
- Dispositivos pessoais não são permitidos para armazenamento de dados corporativos, a menos que expressamente autorizados pelo departamento de TI.

#### 8.2. Criptografia de Dados

Todos os dados armazenados em dispositivos USB devem ser criptografados usando métodos aprovados pelo departamento de TI.

#### 8.3. Restrições de Uso

- O uso de dispositivos USB não é permitido para transferência de dados confidenciais para fora da rede corporativa, a menos que expressamente autorizado pelo departamento de TI.
- Não é permitido compartilhar dispositivos USB entre computadores pessoais e corporativos.
- Os funcionários não devem usar dispositivos USB em computadores públicos ou não confiáveis.
- É proibido o uso de dispositivos USB para fins não relacionados ao trabalho.

#### 8.4. Monitoramento e Auditoria

- A TI realizará auditorias periódicas para verificar o cumprimento desta política.
- Todos os funcionários devem cooperar com as auditorias e fornecer informações necessárias quando solicitado.

#### 8.5. Consequências para o Não Cumprimento

- O não cumprimento desta política pode resultar em ação disciplinar, incluindo advertências, suspensão ou demissão, dependendo da gravidade da violação.
- As violações graves podem ser encaminhadas às autoridades competentes.

### 9. REGISTRO DE ALTERAÇÕES

Revisão	Alteração	Data	Responsável
A	Criação	25/01/23	Vitor Faustino
B	Revisão periódica a cada 02 anos	11/02/25	Vitor Faustino