	<b>INSTRUÇÃO DE OPERAÇÃO</b>		<b>ITO-274</b>
	Título:		Revisão: <b>B</b>
	<b>DEVOLUÇÃO E DESTRUIÇÃO DE INFORMAÇÕES DE PESSOAIS</b>		Página: <b>1 de 2</b>
	Departamento: <b>T.I</b>		Data de efetivação: <b>12/02/25</b>
Elaborador	Revisor	Aprovador	
Vitor Faustino	André Munerato	Carina Affonso	

## 1. OBJETIVO

Garantir que as informações pessoais coletadas durante a prestação de serviços sejam adequadamente devolvidas ou destruídas para proteger a privacidade dos indivíduos.

## 2. REFERÊNCIAS

NBR ISO/IEC 27001.  
NBR ISO/IEC 27002.  
NBR ISO/IEC 27005.  
ITO-259 Classificação da informação.  
FO-405 destruição de dados Pessoais.  
PO-15 Política de Proteção de dados Pessoais.  
PO-16 Procedimento de Incidentes de Segurança.

## 3. ABRANGÊNCIA

Esta Política se aplica:

A todos os usuários (sócios, prepostos, empregados, estagiários, aprendizes e contratados, prestadores de serviço) que utilizam as informações da ORGANIZAÇÃO;

A todas as organizações que compõem o Grupo da 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.

**Encarregado de Dados:** Pessoa designada a controlar os dados.

## 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

- **Usuário:** Agentes externos ao sistema ou pessoas que se utilizam dos recursos, serviços e/ou estruturas de tecnologia.
- **Senha/Autenticação:** palavra-passe, ou ainda palavra-chave ou password, é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.
- **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

### 8.1. Identificação de Dados Pessoais:

- Determine quais informações pessoais foram coletadas durante a prestação de serviços. Isso pode incluir uma lista detalhada dos tipos de informações pessoais, categorias de dados e fontes de dados

	<b>INSTRUÇÃO DE OPERAÇÃO</b>	<b>ITO-274</b>
	Título:	Revisão: <b>B</b>
	<b>DEVOLUÇÃO E DESTRUIÇÃO DE INFORMAÇÕES DE PESSOAS</b>	Página: <b>2 de 2</b>

- Designe um encarregado de dados para supervisionar o processo.

## 8.2. Avaliação de Necessidade de Devolução:

- Avalie se é necessário devolver informações pessoais aos titulares ou se a destruição é apropriada.
- Considere as obrigações contratuais e regulatórias que podem afetar a decisão.

## 8.3. Cópia de Segurança (Backup):

- Antes de qualquer ação ser tomada, faça uma cópia de segurança segura de todas as informações pessoais identificadas. Armazene essas cópias de segurança em um local seguro e com acesso restrito.

## 8.4. Devolução de Dados (se aplicável):

- Se a devolução for necessária, siga os procedimentos específicos para garantir que isso seja feito de maneira segura e de acordo com as regulamentações de privacidade aplicáveis.
- Mantenha registros das devoluções realizadas.

## 8.5. Destruição de Dados:

- Se a destruição for necessária, siga as políticas e procedimentos específicos de destruição segura da empresa, que podem incluir:
- Destruição física de documentos: Triture, queime ou destrua fisicamente os documentos que contenham informações pessoais.
- Destruição de dados eletrônicos: Utilize um software de destruição de dados para sobrescrever ou destruir completamente os dados em dispositivos eletrônicos.
- Documente a destruição de dados, incluindo datas, métodos e responsáveis através do F0-405 Destruição de dados Pessoais

## 8.6. Registro da Ação:

- Mantenha registros detalhados de todas as ações realizadas, incluindo datas, horários, responsáveis e descrição das atividades realizadas. Isso é importante para fins de auditoria e conformidade.

## 8.7. Comunicação Interna e Externa:

- Comunique internamente à equipe relevante sobre a conclusão do processo de devolução ou destruição e qualquer ação subsequente que deva ser tomada.
- Comunique externamente aos titulares de dados, quando aplicável, sobre a devolução de seus dados.

## 8.8. Revisão e Atualização:

- Periodicamente, reveja e atualize este procedimento de acordo com as mudanças nas regulamentações de privacidade e nas políticas da empresa.

## 8.9. Treinamento:

- Certifique-se de que os funcionários envolvidos sejam treinados nas políticas e procedimentos relacionados à devolução e destruição de informações pessoais.

## 9. REGISTRO DE ALTERAÇÕES

Revisão	Alteração	Data	Responsável
A	Criação	25/01/23	Vitor Faustino
B	Revisão periódica a cada 02 anos	12/02/25	Vitor Faustino