	INSTRUÇÃO DE OPERAÇÃO		ITO-260
	Título:		Revisão: B
	SEGURANÇA E PROTEÇÃO DA INFORMAÇÃO		Página: 1 de 3
	Departamento: T.I		Data de efetivação: 01/09/24
Elaborador	Revisor	Aprovador	
Vitor Faustino	André Munerato	Carla Garcia	

1. OBJETIVO

Descrever o tratamento das informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da ORGANIZAÇÃO.

As orientações aqui apresentadas são os princípios fundamentais e representam como a ORGANIZAÇÃO exige que a informação seja utilizada.

2. REFERÊNCIAS

- NBR ISO/IEC 27001
- NBR ISO/IEC 27002
- NBR ISO/IEC 27005
- ITO-96 Política de uso aceitável da internet
- ITO-259 Classificação da informação
- ITO-261 Uso do Correio eletrônico
- ITO-265 Utilização do Ambiente Internet pelo Usuário

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.

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

- **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.

	INSTRUÇÃO DE OPERAÇÃO	ITO-260
	Título: SEGURANÇA E PROTEÇÃO DA INFORMAÇÃO	Revisão: B
		Página: 2 de 3

7. EPI

N/A

8. DESCRIÇÃO DA ATIVIDADE

8.1. O bem da informação

- A informação utilizada pela ORGANIZAÇÃO é um bem que tem valor.
- A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e audibilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

8.2. O gestor da informação (GI)

- Cada informação deverá ter seu gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.
- O GI é o responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

8.3. Confidencialidade da informação

- O GI classificará o nível da confidencialidade e sigilo da informação baseando-se nos critérios estabelecidos na ITO-259.
- A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dela.

8.4. Utilização da informação e recursos


- A liberação do acesso da informação para os usuários será autorizada pelo GI, que considerará a necessidade de acesso do usuário e o sigilo da informação para a realização dos objetivos da ORGANIZAÇÃO.
- O acesso da informação deve ser autorizado apenas para os usuários que necessitam da mesma para o desempenho das suas atividades profissionais para a ORGANIZAÇÃO.
- Cada usuário deve acessar apenas informações e os ambientes previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma falta grave.
- O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Este acesso acontece através da identificação e da autenticação do usuário. Os dados para a autenticação do usuário devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação.
- Os recursos de tecnologia da ORGANIZAÇÃO disponibilizados para os usuários têm como objetivo a realização de atividades profissionais. A utilização dos recursos da ORGANIZAÇÃO com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da ORGANIZAÇÃO.

8.5. Proteção da informação

- Toda informação da ORGANIZAÇÃO deve ser protegida para que não seja alterada, acessada e destruída indevidamente.
- Os locais onde se encontram os recursos da informação devem ter proteção e controle de acesso físico compatível com seu nível de criticidade.

8.6. Continuidade do uso da informação

- Toda informação utilizada para o funcionamento da ORGANIZAÇÃO deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a existência de planos de continuidade de negócio.
- A criação das cópias de segurança deve considerar os aspectos legais históricos, de auditoria e de recuperação do ambiente.
- Os recursos tecnológicos, de infraestrutura e ambientes físicos onde são realizadas as atividades operacionais do negócio da ORGANIZAÇÃO devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade de negócio.
- A definição e implementação das medidas de prevenção e recuperação, para situações de desastres e contingência, devem ser efetuadas de forma permanente e devem contemplar recursos de

	INSTRUÇÃO DE OPERAÇÃO	ITO-260
	Título: SEGURANÇA E PROTEÇÃO DA INFORMAÇÃO	Revisão: B
		Página: 3 de 3

tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da diretoria gestora dos recursos, contando com o apoio e validação da área de segurança da informação.

8.7. Computação pessoal e móvel

- As informações estruturadas e sistemas da ORGANIZAÇÃO somente serão utilizados em recursos da própria.
- É proibido o uso de equipamentos pessoais para acessar informações estruturadas e sistemas corporativos da ORGANIZAÇÃO.

8.8. Correio eletrônico

- O uso do correio eletrônico deve ocorrer conforme ITO-261.
- As mensagens do correio eletrônico disponibilizado para os usuários obrigatoriamente devem ser escritas em linguagem profissional e que não comprometa a imagem da ORGANIZAÇÃO, e que não vá de encontro à legislação vigente e nem aos princípios éticos da ORGANIZAÇÃO. Cada usuário é responsável pela conta de correio eletrônico que lhe foi disponibilizada pela ORGANIZAÇÃO.
- O conteúdo do correio eletrônico de cada usuário pode ser acessado e monitorado pela ORGANIZAÇÃO quando em situações que ponha em risco sua imagem, seu negócio ou sua lucratividade. O usuário não deve ter expectativa de sigilo da sua conta de correio eletrônico disponibilizado pela ORGANIZAÇÃO para seu uso profissional.

8.9. Ambiente de Internet

- O ambiente de Internet deve ser usado para o desempenho das atividades profissionais do usuário para a ORGANIZAÇÃO conforme ITO-265 e ITO-96.
- Sites que não contenham informações que não agreguem conhecimento profissional e para o negócio não devem ser acessados.
- Os acessos realizados nesse ambiente são monitorados pela ORGANIZAÇÃO com o objetivo de garantir o cumprimento dessa política.

8.10. Redes Sociais

Os usuários obrigatoriamente devem seguir as regras de uso de Serviço de Rede Social descrito na norma específica.

8.11. Documentação

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que a ORGANIZAÇÃO continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

8.12. Penalidades

O não cumprimento das regras estabelecidas neste documento pode acarretar sanções administrativa e/ou contratuais, podendo chegar à demissão de funcionário ou rescisão de contrato de prestação de serviço.

9. REGISTRO DE ALTERAÇÕES

Revisão	Alteração	Data	Elaborador
A	Criação	25/08/22	Vitor Faustino
B	Revisão periódica a cada 2 anos	01/09/24	Vitor Faustino