POLÍTICA DE SENHA

1. FINALIDADE

Estabelecer diretrizes sobre complexidade de senhas que deverão ser seguidas por todos os colaboradores da Itaesbra.

1.1. DA ABRANGÊNCIA

Colaboradores, funcionários, prestadores de serviços e parceiros de negócios da Itaesbra.

Para fins do disposto neste documento, os termos:

- "Organização" contemplará todos os espaços físicos e lógicos, atividades, materiais, recursos humanos e financeiros diretamente relacionados com os segmentos de negócios mantidos pela Itaesbra.
- "Colaboradores" contemplará todos os funcionários, prestadores de serviços, menores aprendizes, trainees, estagiários, parceiros de negócios e fornecedores da Itaesbra.

Este documento - Política de Senha - também se aplica, quando pertinente for, ao relacionamento com entidades terceiras como Instituições Acreditadoras Credenciadas (IAC) pela Organização Nacional de Acreditação (ONA) no Brasil.

1.2. DAS REFERÊNCIAS LEGAIS E NORMATIVAS

- ABNT NBR ISO/IEC 27001:2022 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.
- ABNT NBR ISO/IEC 27701:2019 —Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
- Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

1.3. DOS TERMOS E DEFINIÇÕES

Os Termos, Expressões e Definições utilizados neste documento estão conceituados no documento, Política de Segurança da Informação (PSI): "IEB-SGSI-001 – Termos, Expressões e Definições".

2. RESPONSABILIDADES

- Da área de Tecnologia da Informação (TI)
  - Solicitar aos Gestores de Área e/ou Proprietários informações que sigam a orientação para a adequada criação/alteração de senhas;
  - Garantir a atualização deste documento: "IEB-SGSI-007 – Política de Senha".
- Dos Gestores da área / Equipe / Setor
  - Solicitar de Tecnologia da Informação (TI) a inclusão e/ou adequação de termos pertinentes à Política de Senha;
  - Responder às solicitações de Tecnologia da Informação (TI) acerca das informações que permitam a compreensão e adequada sobre complexidade de senha;
  - Garantir que todos os Colaboradores pertinentes às suas respectivas áreas tenham conhecimento, pratiquem e respeitem as diretrizes dispostas neste documento.

4. ENTRADAS

- Entrada 1 – Receber, analisar, aprovar e/ou vetar sobre a complexidade de senhas utilizadas pelos colaboradores.

5. SAÍDAS

- Saída 1 - Solicitação de inserção e/ou adequação de documentação pertinente à Política de Senhas.

6. PROCEDIMENTOS

Esta seção contém diretrizes sobre os procedimentos cabíveis e pertinentes à complexidade de senhas compreendidas e adotadas pela Itaesbra.

6.1 Complexidade de Senha Windows e Logix:

Os requisitos de complexidade de senha descritos abaixo são aplicados quando ocorre a criação de senha e/ou alteração dela.
As senhas deverão ter:

- Mínimo de 8 (sete) caracteres;
- Caracteres maiúsculos (A a Z)

- Caracteres minúsculos (a a z)
- Base 10 dígitos (0 a 9)
- Caracteres não alfabéticos (por exemplo, $, #, %)

Para login no Windows as senhas não deverão conter:

- Nome da conta do usuário que excedam dois caracteres consecutivos;
- Partes do nome completo do usuário que excedam dois caracteres consecutivos;

6.2. Validade das senhas;

A senha tem validade de 180 dias, após este período a senha expira e obriga o usuário a cadastrar uma nova senha.

6.3. Monitoramento de histórico de senhas

A Itaesbra utiliza o Active Directory para monitorar/verificar a complexidade das senhas, bem como além verificar a utilização recente da mesma senha. Todo o processo ocorre com base no número de senhas anteriores que foram armazenadas.

Para além disso, a complexidade de senhas é baseada nos recursos de gerenciamento de senhas do Active Directory (AD) através das Diretivas de Segurança. Para tanto, a política de senhas mantida sob o AD assegura caracteres complexos, tamanho mínimo de senha, tempo mínimo e máximo para expiração da senha, histórico das duas últimas senhas, e, log, através do Visualizador de Eventos do Windows Server - Active Directory: Segurança - para acompanhar tentativas sem sucesso de logon utilizando senha incorreta.

6.4. Senha do ERP.

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**
1	29/07/24	ENCARREGAOO PELA PROTEÇÃO DE DADOS (DPO)	Publicação inicial	Julio Cezar