1 . FINALIDADE

Estabelecer diretrizes para o uso de criptografia nos sistemas computacionais de propriedade da ITAESBRA.

2. INTRODUÇÃO

Este documento contém diretrizes estabelecidas pela ITAESBRA para o uso de criptografia, com o objetivo de fornecer um guia claro e organizado que orienta sobre o uso correto e seguro da criptografia em todas as atividades relacionadas à segurança da informação.

2.1 . DA ABRANGÊNCIA

CSIPD, ISO, Operação.

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;
- Colaborador(es): contemplará todos os funcionários, prestadores de serviços, menores aprendizes, trainees, estagiários, parceiros de negócios e fornecedores da ITAESBRA.

O conteúdo disposto neste documento aplica-se à Organização da ITAESBRA, devendo ser em sua totalidade observado por Colaboradores sob pena de violação de regulamentos internos.

Este documento - Política de Uso de Criptografia - também se aplica, quando pertinente for, ao relacionamento com Autoridades, Entidades, e/ou Instituições terceiras como a Autoridade Nacional de Proteção de Dados (ANPD), Instituições Acreditadoras Credenciadas (IAC) pela Organização Nacional de Acreditação (ONA) no Brasil.

2.2. 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 27002:2022 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação.
- ABNT NBR ISO/IEC 27003:2022 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações
- ABNT NBR ISO/IEC 27701 :2022 —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).

2.3. DOS TERMOS E DEFINIÇÕES

Os Termos, Expressões e Definições utilizados neste documento estão conceituados no documento, Política de Segurança da Informação – Termos, Expressões e Definições".

3. RESPONSABILIDADES

- Da área de TI e SI
  - Analisar em conjunto com colaboradores de expertise suficiente sobre o assunto criptografia, a suficiência e/ou viabilidade de uso dos controles/recursos aplicados e instituídos;
  - Solicitar aos Gestores de Área e/ou Proprietário do Recurso de TI/Colaborador, informações que permitam a adequada compreensão para deliberar sobre o uso de criptografia;
  - Garantir a atualização deste documento: "Política de Uso de criptografia".
- Dos Gestores de Área / Equipe / Setor
  - Solicitar ao TI e SI informações sobre o funcionamento/uso e/ou instalação dos recursos pertinentes a criptografia, bem como informar o ISO sobre possíveis problemas que possam ter surgido durante o uso;
  - Garantir que todos os colaboradores pertinentes às suas respectivas áreas tenham conhecimento, pratiquem e respeitem as diretrizes dispostas neste documento.

- Da equipe de TI
  - Aplicar e manter todos os recursos necessário para o correto funcionamento dos recursos pertinentes a criptografia;
  - Proteger a integridade e confidencialidade dos dados, garantindo que os dados transferidos não sejam adulterados e que não sejam lidos ou interpretados por partes não autorizadas;
  - Gerenciar e proteger as chaves criptográficas. Isso inclui o armazenamento seguro, distribuição e rotação periódica das chaves para garantir a segurança contínua, além de garantir que elas estejam protegidas contra acessos não autorizados;
  - Monitorar o tráfego de rede para detectar atividades suspeitas ou tentativas de comprometer a criptografia.
- Da equipe de TI
  - Prestar suporte aos colaboradores que encontrarem dúvidas ou problemas relacionados à criptografia, como configuração de VPNs, uso de certificados digitais, ou aplicação de criptografia de arquivos;
  - Identificar e resolver problemas relacionados à criptografia, como problemas de autenticação, erros de certificados digitais ou problemas de acesso a sistemas criptografados;
  - Auxiliar no gerenciamento de senhas e chaves criptográficas, incluindo a recuperação de senhas perdidas e a orientação sobre como proteger suas chaves;
  - Ajudar na obtenção e renovação de certificados digitais, bem como solucionar problemas de autenticação ou validação relacionados a esses certificados;
  - Ajudar na identificação e relato de incidentes de segurança relacionados à criptografia, como tentativas de quebrar a criptografia, ataques ou qualquer atividade suspeita.

4. ENTRADAS

- Entrada 1 - E-mail, ligação telefônica, SMS, Mensagem por serviço de mensageria: WhatsApp, SAVI para solicitação de atualização do documento/PSI, bem como para deliberação sobre Diretrizes/Canais de Comunicação pertinentes ao uso de criptografia.

5. SAÍDAS

- Saída 1 - E-mail, ligação telefônica, SMS, Mensagem por serviço de mensageria: WhatsApp, SAVI para responder/atender à solicitação de atualização do documento/PSI e/ou sobre a deliberação de Diretrizes/Canais de Comunicação pertinentes ao uso de criptografia.

6. PROCEDIMENTOS

Ativação da criptografia via recurso do próprio Windows chamado bitlocker, é salvo uma cópia das chaves de criptografia de cada equipamento no diretório de ti, zipado e protegido por senha.

7. REGISTROS

Controle de Revisão do Documento				
Nº	**Data**	**Elaborado por**	**Histórico da Revisão**	**Revisado por**
00	05/08/23	DPO	Publicação inicial	Julio Cezar Nicolosi