1. OBJETIVO

- Assegurar que os recursos do parque tecnológico e o uso de dados estejam compatíveis com com o nível de segurança exigido pela FMSA e pelos órgãos reguladores e orientar a definição de normas e procedimentos específicos de segurança da informação.
- Garantir que as informações e dados sob propriedade da FMSA estejam gerenciadas e protegidas contra roubo, fraude, espionagem, perda e quaisquer outras ameaças, tornam-se objetivos da cibersegurança:

Confidencialidade: é necessário garantir que os dados de informação devem ser restritos e ter garantia que serão acessíveis apenas pessoas autorizadas;

Integridade: é necessário garantir que os dados e as informações devem ser exatos e sem modificações indevidas – com ou sem intenção;

Disponibilidade: é necessário garantir que as pessoas autorizadas a tratar as informações e dados tenham acesso ao seu conteúdo e possam consultá-las a qualquer momento.

2. CAMPO DE APLICAÇÃO

Aplicar a todos os colaboradores, gestores, representantes, fornecedores, parceiros e terceiros.

3. SIGLAS

- CGPI – Comissão de Gestão de Plano de Integridade
- FMSA – Fundação Manoel da Silva Almeida
- CTI – Cibersegurança e Técnologia da Informação

4. INSTRUÇÕES

Definições

- Software: o conjunto de instruções e dados processados nos servidores e computadores;
- Backup: cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais;
- Mídias removíveis: são ferramentas que permitem não só a a leitura como também gravação de dados como por exemplo: cd, dvd, disquete, pen drive, cartão de memória entre outros;
- Acesso Remoto: modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna.
- Firewall dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- Informação de propriedade da FMSA - toda informação sobre a FMSA , suas filiais e seus colaboradores, fornecedores, terceiros, clientes e diretores.

Diretrizes

- Proteger toda informação – online ou offline - que seja propriedade da FMSA de qualquer ameaça que possa comprometer sua confidencialidade, integridade ou disponibilidade;
- Compatibilizar a proteção de dados com as operações e complexidade de seus produtos;
- Promover a cultura de cibersegurança e proteção de dados a todos seus integrantes e interessados;
- Gerenciar a cibersegurança de forma prospectiva em conjunto com a proteção de dados, atuando com procedimentos e controles que reduzam sua vulnerabilidade a falhas e incidentes;

- Utilizar qualquer informação gerada, tratada ou compartilhada apenas se autorizada;
- Contratar serviços relevantes, fornecedores e terceiros que atuem no processamento e armazenamento de dados que obedeção, além do estipulado na Política de Relacionamento com Fornecedores e Terceiros, às disposições específicas da orientação das Normas de Contratos de Processamento e Armazenamento de Dados e de Computação em Nuvem;
- Tratar incidentes relativos ao sistema cibernético e de dados e definir protocolos de ação para cenários de interrupção dos serviços de processamento e armazenamento de dados e de computação em nuvem.

Normas de Contratação de Serviços de Processamento e Armazenamento de Dados em Nuvem

- Observar a contratação com aderência à estratégia, apetite e gestão de riscos
- Assegurar que o potencial prestador de serviço tenha capacidade de fornecer o produto/serviço dentro das especificações técnicas bem como garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e informações processados ou armazenados;
- Assegurar que o potencial prestador de serviço esteja em condições de cumprir a legislação vigente e fornecer à FMSA, a qualquer tempo, o acesso aos dados e informações a serem processados ou armazenados;
- Documentar a diligência realizada para contratação do prestador de serviço e disponibilizar tais relatórios à unidade responsável pela gestão de riscos;
- Garantir que o contrato firmado entre as partes apresente de maneira clara a adoção de medidas de segurança para transmissão e armazenamento de dados, além da manutenção da segregação de dados e controle de acesso para proteção de informações aos usuários;

- Garantir que o contrato firmado entre as partes apresente de maneira clara as cláusulas, em caso de extinção, que versam sobre a transferência de dados e informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência.

Plano de Ação e de Resposta a Incidentes Cibernéticos

- Mapeamento dos principais incidentes, tanto observado em base histórica quanto incidentes de probabilidade significativa;
- As rotinas, os procedimentos, os controles e a tecnologia empregada na prevenção e na resposta aos incidentes mapeados;
- Produção de relatório anual onde conste os incidentes registrados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da Cibersegurança.

Divulgação da Política de Cibersegurança e Proteção de Dados:

Esta política deve ser divulgada aos colaboradres, fornecedores e terceiros que atuem na FMSA e suas filiais com linguagem clara, acessível e compatível as funções desempenhadas.

Exceções

Fica permitido, sem configurar quebra de sigilo ou confidencialidade, o trânsito de informações com o Banco Central do Brasil, Receita Federal, Poder Judiciário, Agência Nacional de Proteção de Dados, PROCON, representantes da FMSA devidamente qualificados.

5. REFERÊNCIA

BRASIL. Lei nº 13.709/2018, de 14 de agosto de 2018, Lei Geral de Proteção de Dados. Diário Oficial da União - Seção 1 - 15/8/2018, Página 59 (Publicação Original).

Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html>. Acesso em: 9 fev. 2023.

BRASIL. Lei nº 9.609/1998, de 14 de agosto de 2018, Lei de Software. Diário Oficial da União - Seção 1 - 1998, Página 659 Vol. 1 (Publicação Original). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 9 fev. 2023.

BRASIL, Banco Central. Resolução nº 4.658/18, de 26 de abril de 2016, Política De Segurança Cibernética. Disponível em: < https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em:9 fev. 2023.

http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 9 fev. 2023.

ABNT, Associação Brasileira de Normas Técnicas, ABNT NBR ISSO 27000, jun. de 2005, Sistema de Gestão da Segurança da Informação. Disponível em: < https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip>. Acesso em: 9 fev. 2023.

5.HISTÓRICO

PUBLICAÇÃO INICIAL	ALTERAÇÕES
Data: 16/02/2023 **Responsável: Thallys Yuri Oliveira Santiago** **Versão:** 00	Esta versão está sendo considerada 00 devido alteração da estrutura dos documentos e após implantação do Plano de Integridade em 11/2022 e avaliação dos riscos nos subsequentes.
VERSÃO ANTERIOR	**ALTERAÇÕES**
Data: **Responsável:** **Versão:**	
VERSÃO ATUAL	**ALTERAÇÕES**
Data: **Responsável:** **Versão:**	