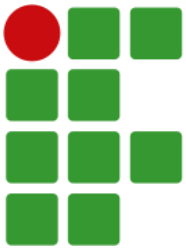

INSTITUTO FEDERAL
Sertão Pernambucano

PLANO DE AÇÃO
DE
SEGURANÇA DA INFORMAÇÃO

Petrolina/PE

2021

Sumário

1 – APRESENTAÇÃO

A Política de Segurança da Informação (PSI) do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF SERTÃO-PE), instituída pela Resolução n. 24 do Conselho Superior de 10 de agosto de 2020, estabelece diretrizes e critérios suficientes à implementação da Segurança da Informação, reconhecida como ativo valioso e recurso fundamental para que a instituição desempenhe suas atribuições.

A Segurança da Informação envolve múltiplos aspectos da Instituição, desde os locais onde a informação é guardada até os recursos humanos e tecnológicos. Englobam processos de trabalho, relação com fornecedores e prestadores de serviço, uso adequado das ferramentas e serviços de tecnologia da informação, cuidados com o ambiente de trabalho e publicação de normativas. Para a gestão da Segurança da Informação foi instituído o Comitê Gestor de Segurança da Informação (CGSI) com a finalidade primordial de assessorar a implantação das ações de segurança da informação.

Este plano de ação visa o planejamento e a definição de ações necessárias para a promoção e fortalecimento da Segurança da Informação do IF SERTÃO-PE, no biênio 2021-2022.

2 – JUSTIFICATIVA

A elaboração deste plano alinha-se ao objetivo estratégico (OB3) de Promover a Segurança da Informação e Comunicação descrito no Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) da Instituição, atendendo a necessidade de adoção de um plano de ações voltadas à Segurança da Informação.

As ações propostas neste documento seguem as necessidades apontadas pelo Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) na promoção e manutenção da Segurança da Informação do IF SERTÃO-PE. Também elas são advindas de recomendações das normas e boas práticas nacionais e internacionais.

3 - DOCUMENTOS DE REFERÊNCIA

I – Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) do IF SERTÃO-PE, 2019-2023;

II – Plano Diretor de Tecnologia da Informação (PDTIC) do IF SERTÃO-PE, 2019-2021;

III – Plano de ação em segurança da informação, Câmara dos Deputados, Comitê Gestor de Segurança da Informação. – Brasília: Câmara dos Deputados, Edições Câmara, 2014;

IV – ABNT NBR ISO/IEC 27001:2013 - Código de prática para controles de segurança da informação;

V – ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;

VI - Instrução Normativa nº 1, de 27 de maio de 2020, dispõe sobre a sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

4 - OBJETIVOS

- Promover as ações necessárias à implementação e manutenção da segurança da informação;
- Estabelecer atividades necessárias à efetiva concretização da segurança da informação.

5- PLANO DE AÇÃO

5.1 - Regulamentar a Política e o Plano de Backup e Recuperação de dados

- **Descrição:** A Política de backup é um documento elaborado para guiar a Instituição nos processos que permitem salvaguardar os dados armazenados pelos sistemas, garantindo guarda, proteção e recuperação. Ela define criteriosamente o modo e a periodicidade das cópias de segurança e sua efetiva restauração. Os procedimentos de backup e restauração são essenciais para assegurar a continuidade do negócio e a consequente prestação de serviços.
- **Ação 1:** Instituir Política para garantir a segurança, a proteção e a disponibilidade das informações.
- **Indicador 1:** Número de políticas implementadas na Instituição.
- **Meta 1:** Uma política instituída.
- **Ação 2:** Instituir Plano de Backup e Recuperação de Dados para garantir a segurança, a proteção e a disponibilidade das informações.
- **Indicador 2:** Número de planos de backup implementados na Instituição.
- **Meta 2:** Implementar 8 planos de backup (um por unidade organizacional institucional).
- **Resultados esperados**: Implantação de mecanismos de guarda e recuperação de dados e informações institucionais em casos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças; Redução de ocorrência de incidentes de Segurança da Informação; Redução dos custos decorrentes de incidentes de Segurança da Informação; Conformidade da instituição com leis, regulamentos, normas e recomendações dos órgãos de controle.

5.2 - Normatizar a Classificação e o Tratamento das Informações

- **Descrição:** A classificação e o Tratamento das Informações tornam possível a adoção de medidas de proteção proporcionais à importância ou à reserva de acesso que caracteriza uma informação específica. Entre os vários critérios aplicáveis a eles, dois são especialmente importantes do ponto de vista da Segurança da Informação: o valor da informação e seu grau de sigilo. A classificação e o tratamento da informação quanto ao seu

livre acesso, ou à restrição de acesso, ou ainda quanto ao seu grau de sigilo é condição necessária para que, nos casos aplicáveis, se possa preservar sua confidencialidade.

- **Ação:** Instituir norma que estabeleça critérios, procedimentos e responsabilidades para a classificação e tratamento das informações segundo o grau de proteção requerido.
- **Indicador:** Número de normas de classificação instituídas na Instituição.
- **Meta:** Uma Norma Complementar de Classificação e Tratamento das Informações instituídas na instituição.
- **Resultados esperados:** Proteção das informações classificadas na proporção de seu grau de sigilo ou de restrição de acesso; Conscientização dos colaboradores quanto à necessidade de proteger os ativos de informação; Fortalecimento da cultura de Segurança da Informação; Redução de ocorrência de incidentes de Segurança da Informação; Conformidade da instituição com leis, regulamentos, normas e recomendações dos órgãos de controle.

5.3 Realizar a Gestão de Incidentes de Segurança da Informação

- **Descrição**: Um incidente de Segurança da Informação tem uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. A sua gestão proporciona que tais eventos sejam identificados para permitir a tomada de ação e resposta mais rápida e eficiente.
- **Ação 1:** Instituir a norma que estabeleça critérios, procedimentos e artefatos para o processo de Gestão de Incidentes de Segurança na Informação.
- **Indicador 1:** Número de Normativa de Gestão de Incidentes de Segurança da Informação instituída.
- **Meta 1:** Uma norma de Gestão de Incidentes de Segurança na Informação instituída.
- **Ação 2:** Formalizar o processo de Gestão de Incidentes de Segurança na Informação.
- **Indicador 2:** Número de processo de Gestão de Incidentes de Segurança na Informação.

- **Meta 2:** Um processo de Gestão de Incidentes de Segurança na Informação formalizado.
- **Ação 3:** Sistematizar o processo de Gerenciamento destes eventos.
- **Indicador 3:** Número de Sistematização realizadas no processo de Gerenciamento destes eventos.
- **Meta 3:** Um processo de Gestão de Incidentes de Segurança na Informação sistematizado.
- **Resultados esperados:** Redução do risco de incidentes que possam resultar em perda, dano, indisponibilidade ou acesso indevido à informação; aprimoramento da segurança e disponibilidade dos serviços e sistemas; conformidade da instituição com leis, regulamentos, normas e recomendações dos órgãos de controle.

5.4 Estimular a Conscientização, treinamento e aculturamento sobre Segurança da Informação.

- **Descrição:** As ações de conscientização, treinamento e aculturamento dos usuários sobre Segurança da Informação são iniciativas fundamentais para torná-los cientes das suas responsabilidades e conhecedores das práticas e métodos aplicáveis à proteção da informação. É importante que os conceitos e a relevância da Segurança da Informação passem a fazer parte da cultura organizacional por uma campanha permanente que promova essa transformação. Nessas atividades os usuários terão conhecimento dos regulamentos que estão em implantação (ou já implantados) em segurança da informação; entenderão esses regulamentos e serão apresentados às suas responsabilidades perante o Processo Organizacional de Segurança da Informação.
- **Ações:** Oferecer cursos, eventos e campanhas regularmente para que todos os usuários recebam o treinamento adequado para a sua conscientização e para a sua capacitação em relação às suas responsabilidades em relação à segurança da informação.
- **Indicadores:** Quantidade de cursos, eventos, treinamentos e campanhas de conscientização realizadas;
- **Meta 1:** 1 curso sobre Segurança da Informação por ano.
- **Meta 2:** 1 evento sobre Segurança da Informação por ano.
- **Meta 3:** 1 campanha sobre Segurança da Informação por ano.

- **Resultados esperados:** Usuários conscientes da importância de se preservar a Segurança da Informação em seus processos de trabalho e treinados em como mantê-la; Condutas adequadas e comportamentos desejáveis dos usuários em relação à preservação da Segurança da Informação; Redução da ocorrência de incidentes de Segurança da Informação.

5.5 Atualizar das Normas de Uso dos Recursos Computacionais

- **Descrição:** A padronização torna a utilização segura, consciente e responsável dos recursos de tecnologia da informação e comunicação.
- **Ações:** Atualizar normas que estabeleçam as regras de uso, no ambiente organizacional, dos recursos Computacionais e de Comunicações essenciais ao desempenho das atividades exercidas no IF SERTÃO-PE.
- **Indicador:** Número de normas atualizadas.
- **Meta:** 4 normas atualizadas por ano (Norma de Acesso à Internet; Norma de Regulamentação da utilização das estações de trabalho em rede, Norma de Regulamentação que estabelece regras e diretrizes para os subdomínios, sítios e serviços eletrônicos na internet, Norma de Regulamentação da utilização dos laboratórios de Informática).
- **Resultados esperados:** Uso consciente e seguro dos recursos; Conscientização dos colaboradores quanto à necessidade de proteger os ativos de informação; Fortalecimento da cultura de Segurança da Informação; Redução de ocorrência de incidentes de Segurança da Informação; conformidade da instituição com leis, regulamentos, normas e recomendações dos órgãos de controle.

6 – ACOMPANHAMENTO DAS AÇÕES

O Comitê Gestor de Segurança da Informação propõe que seja feito, trimestralmente, o acompanhamento das ações aqui recomendadas, por meio de solicitação de informações às equipes responsáveis por desenvolver as ações propostas neste plano.

7 – CONSIDERAÇÕES FINAIS

Considerando os benefícios decorrentes das ações aqui propostas, o Comitê Gestor de Segurança da Informação manifesta a expectativa de que a Administração acolha este Plano de Ação em Segurança da Informação, reconheça o seu caráter estratégico para os processos de trabalho da Instituição.

Andson da Silva Rodrigues: 07396115426

Assinado digitalmente por Andson da Silva Rodrigues: 07396115426
Localização: Petrolina/PE
Data: 2021.03.15 16:21:40-03'00'
Foxit Reader Versão: 10.1.1

Andson Da Silva Rodrigues
Gestor de Segurança da Informação