1. UNIDADES RELACIONADAS

A Política de Segurança da Tecnologia da Informação compreende diretamente aos Servidores que desempenham suas atividades na Unidade de Tecnologia da Informação e indiretamente à totalidade das Unidades da Secretaria de Estado da Retomada.

2. OBJETIVO

A Política de Segurança da Tecnologia da Informação, tem como objetivo estabelecer critérios de segurança para acesso e armazenamento das informações, a fim de aumentar a segurança do processo interna e externamente, diminuindo a subjetividade permitindo decisões rastreáveis e consistentes.

3. RESPONSABILIDADES

O cumprimento das normas aqui estabelecidas é de responsabilidade da totalidade dos Servidores da Tecnologia da Informação e dos demais Servidores da Secretaria de Estado da Retomada.

4. REFERÊNCIAS E LEGISLAÇÃO RELACIONADA:

- ✓ ISO/IEC 27001 - Norma que define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).
- ✓ ISO/IEC 27002 é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.
- ✓ Decreto n° 9.406/2019 - Programa de Compliance Público
- ✓ Portaria nº 56/2019 - Política de Gestão de Riscos CGE
- ✓ Lei nº 20820/2020 – Instituição da Secretaria de Estado da Retomada.

5. CONCEITO;

A política de segurança da informação (PSI) é um conjunto de padrões, normas e diretrizes a todos os servidores que utilizam infraestrutura de TI da Secretaria de Estado da Retomada, que tem como finalidade, garantir a proteção das informações corporativas contra eventuais ameaças que possam prejudicar sua operação

A PSI carrega o propósito de minimizar riscos de perdas ou violação de qualquer ativo de TI. Essa política protege as informações da Pasta, que poderia causar algum dano intencionalmente ou não.

A PSI visa proteger e garantir os três princípios da segurança da informação – confidencialidade, integridade e disponibilidade. As normas e práticas descritas se relacionam a esses princípios.

A PSI planejada avalia desde riscos à infraestrutura de TI, contra roubos, panes ou desastres naturais, até as ameaças digitais, como malwares, phishing e ransomwares.

6. CONFIDENCIALIDADE DAS INFORMAÇÕES;

A confidencialidade assegura que as informações da Pasta, sejam acessadas apenas por pessoas autorizadas, esse princípio é importante, uma vez que o extravio de informações pode acarretar desde crise de imagem a processos judiciais com grandes prejuízos para a Secretaria.

7. INTEGRIDADE DAS INFORMAÇÕES;

Esse princípio adotado, garante que os dados não sejam alterados ou apagados, de forma a apresentar informações confiáveis, íntegras e verdadeiras.

8. DISPONIBILIDADE DAS INFORMAÇÕES;

O PSI aqui descrito tem como princípio a disponibilidade, em que os dados estão continuamente disponíveis para uso sempre que demandados por alguém com permissão de acesso.

9. ACESSO À INFORMAÇÕES RELEVANTES;

O acesso a informações relevantes é pautado com base na necessidade dos servidores, garantindo acesso as informações e limitando o acesso até sua divulgação seja oportuna.

10. ACESSO AOS ATIVOS E RECURSOS FINANCEIROS;

Tem como objetivo proteger os ativos, patrimonio e produzir dos contábeis confiáveis, garantindo a confiabilidade e precisão das informações.

11. ACESSO AOS REGISTROS CONTÁBEIS;

Acesso a esses registros representa as pessoas que preparam ou manuseiam informações que servem de base para sua elaboração, em circunstâncias que lhes permitem modificar os dados desses registro.

12. SEGURANÇA DO ARMAZENAMENTO E PROTEÇÃO DOS DADOS NO SERVIDOR;

Para manter segura e protegido os dados nos servidores, o controle de acesso, físico ou lógicos, tem como objetivo proteger equipamento, aplicativos e arquivos de dados contra a perda, modificação ou divulgação não autorizada.

13. SEGURANÇA CONTRA AMEAÇAS DIGITAIS;

A proteção dos recursos computacioanais, baseia-se na necessidade de utilizar usuário e senha, para identificar o servidor. A utilização de antivirus e somente permitir aos servidores competentes da área qualquer instalação de programas.

14. BOAS PRÁTICAS DE USO DO E-MAIL CORPORATIVO;

As boas práticas são para manter a boa saúde do e-mail corporativo, através da criação de senha com complexidade alta, limpeza da caixa de e-mail, realizar backups com frequência e reprtar e-mails suspeitos.

15. NORMAS GERAIS PARA USO DE DISPOSITIVOS, INTERNET, INSTALAÇÃO DE SOFTWARES E ACESSO POR DISPOSITIVOS PESSOAIS;

O uso de equipamentos de informática e comunicação, sistemas e informações que são utilizados pelos servidores são para atividades relativas ao cargo exercido. Devendo ter cuidado para não danificar ou prejudicar seu funcionamento. A instalção de software está restrita a equipe de T.I, o acesso por dispositivos pessoais devem atender aos requisitos mínimos de segurança com utilização de firewall e antivirus.

16. PENALIDADES APLICÁVEIS;

As penalidades aplicáveis ao cesso ilícito e repasse de informações institucionais sigilosas, discorrerão conforme a Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos.

NOTA: A Política de Segurança da Tecnologia da Informação foi estabelecida na Instituição da Secretaria de Estado da Retomada, atualmente se encontra em Implantação a descrição formalizada, porém executada e praticada desde a criação do órgão em 04 de agosto de 2020.

17. NOTIFICAÇÕES;

O uso indevido dos equipamentos e instrumentos informatizados devem ter seus acessos suspensos no ato da identificação das desconformidades e notificado ao Superintendente da Unidade e Gerência de Desenvolvimento de Pessoas – GEGDP, para que providências sejam tomadas conforme item16.

18. HISTÓRICO DE REVISÕES

REV. 0:
Emissão inicial – Maio 2021

ELABORADO POR:
Paulo Vitor Machado Ribeiro – Assessor A3 – Coordenador de T.I – Maio 2021

REVISADO POR:
Letícya Fernandes Rezende – Gerente de Apoio e Compras Governamentais – Maio 2021

APROVADO POR:
César Moura – Secretário de Estado - Maio 2021