1. Introdução

Neste relatório, propomos o desenvolvimento de um framework personalizado de segurança e governança de TI, com base nas boas práticas dos frameworks COBIT, ISO/IEC 27001 e NIST Cybersecurity Framework. O objetivo é adaptar esses referenciais amplamente reconhecidos à realidade da nossa organização, promovendo um ambiente tecnológico seguro, alinhado aos objetivos estratégicos e à conformidade regulatória.

2. Objetivos do Framework Personalizado

- Garantir a confidencialidade, integridade e disponibilidade das informações.
- Alinhar a TI aos objetivos de negócio.
- Estabelecer políticas, processos e controles de segurança da informação.
- Promover a melhoria contínua da governança e da segurança de TI.
- Estabelecer uma abordagem baseada em riscos.

3. Fundamentos Utilizados

3.1. COBIT

- Foco na governança de TI e alinhamento estratégico.
- Entrega de valor, gestão de riscos e desempenho.
- Estrutura baseada em domínios como: Avaliar, Dirigir e Monitorar (EDM); Alinhar, Planejar e Organizar (APO); Construir, Adquirir e Implementar (BAI); Entregar, Serviço e Suporte (DSS); e Monitorar, Avaliar e Analisar (MEA).

3.2. ISO/IEC 27001

- Foco na gestão da segurança da informação.
- Implementação de um Sistema de Gestão de Segurança da Informação (SGSI).
- Definição de políticas, controles e análise de riscos baseada no ciclo PDCA.

3.2.1 ISO/IEC 27005:
Complementa a ISO/IEC 27001 ao detalhar a abordagem para a gestão de riscos em segurança da informação. Fornece diretrizes para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos com base em critérios claros.

3.3. NIST Cybersecurity Framework

- Estrutura baseada em 5 funções principais: **Identificar, Proteger, Detectar, Responder e Recuperar**.
- Ênfase na resiliência cibernética e proteção contra ameaças.

4. Estrutura do Framework Personalizado

Abaixo, apresentamos o framework adaptado à realidade da nossa organização:

Função	Objetivo	Práticas Adaptadas	Ferramentas/Controles
Governança	Estabelecer liderança e responsabilidade em segurança de TI	COBIT (EDM), ISO (Política de Segurança)	Comitê de Segurança, Relatórios de Auditoria
Planejamento e Alinhamento	Alinhar a TI à estratégia organizacional	COBIT (APO), NIST (Identificar)	Planejamento Estratégico de TI, Inventário de Ativos
Gestão de Riscos	Avaliar e tratar riscos de segurança	ISO/IEC 27005, NIST (Identificar)	Análise de Risco, Matriz de Impacto x Probabilidade
Segurança Operacional	Implementar e operar controles de segurança	ISO (Anexo A), NIST (Proteger)	Controle de Acesso, Backup, Gestão de Vulnerabilidades
Monitoramento e Resposta	Monitorar e reagir a incidentes de segurança	NIST (Detectar, Responder), COBIT (DSS, MEA)	SIEM, Plano de Resposta a Incidentes
Melhoria Contínua	Aprimorar constantemente a segurança e a governança	ISO (PDCA), COBIT (MEA)	Auditorias Internas, Indicadores de Desempenho

5. Benefícios Esperados

- Redução de riscos e maior proteção contra ameaças cibernéticas.
- Clareza na responsabilidade e tomada de decisão em TI.
- Conformidade com normas e regulamentos.
- Melhoria no desempenho dos serviços de TI.
- Aumento da confiança dos stakeholders.

6. Conclusão

O framework proposto permite que a organização tenha uma abordagem integrada e sob medida para governança e segurança da informação. Ao combinar práticas consolidadas dos frameworks COBIT, ISO/IEC 27001 e NIST CSF, conseguimos adaptar as diretrizes de forma prática e estratégica para o nosso contexto, promovendo segurança, conformidade e alinhamento com os objetivos do negócio.

Links de acessos aos manuais para mais informações:

COBIT(2019): https://www.isaca.org/resources/cobit

NIST: https://www.nist.gov/system/files/documents/2021/09/02/NIST.CSWP_.01162020pt.pdf

ISO/IEC 27001: https://www.iso.org/standard/27001

ISO/IEC 27005: https://www.iso.org/standard/80585.html