IEC/ISO 27001

Instruções

Baseado no IEC/ISO 27001 descreva o Modelo PDCA aplicado aos processos do SGSI idealizando um exemplo prático. Abaixo segue 2 exemplos:

EXEMPLO 1: Um requisito pode significar que violações de segurança da informação não causem sérios danos financeiros e/ou constrangimentos à organização.

EXEMPLO 2: Uma expectativa pode significar que se um incidente grave ocorrer – por exemplo, a invasão da página Internet de comércio eletrônico de uma organização – deveria haver pessoas com treinamento suficiente nos procedimentos apropriados para minimizar o impacto.

**O Modelo PDCA (Plan-Do-Check-Act) é um ciclo de melhoria contínua amplamente utilizado na gestão da segurança da informação, de acordo com o padrão ISO/IEC 27001. Esse modelo ajuda a garantir que os processos do Sistema de Gestão de Segurança da Informação (SGSI) sejam bem planejados, implementados, monitorados e melhorados continuamente.**

**Aqui está um exemplo prático de como o modelo PDCA pode ser aplicado aos processos do SGSI, baseado nos exemplos fornecidos:**

Plan (Planejar)

Definir os objetivos e as metas para o processo em questão, levando em consideração as expectativas e requisitos do exemplo.

* *EXEMPLO 1:* O objetivo deste processo é garantir que as violações de segurança da informação não causem danos financeiros ou constrangimentos à organização. A meta é desenvolver e implementar um conjunto abrangente de medidas de segurança para minimizar o risco de violações de segurança da informação.
* *EXEMPLO 2:* O objetivo deste processo é garantir que a organização esteja pronta para responder efetivamente a incidentes de segurança, minimizando o impacto nos negócios. A meta é desenvolver e implementar um plano de resposta a incidentes que inclua treinamento para as pessoas envolvidas no processo.

# Do (Fazer)

Implementar o plano definido na etapa anterior.

* *EXEMPLO 1:* Implementar medidas de segurança abrangentes, como criptografia de dados, controles de acesso, backups regulares e auditorias de segurança. Alocar recursos suficientes para garantir a eficácia dessas medidas.
* *EXEMPLO 2:* Realizar treinamento para as pessoas envolvidas no processo de resposta a incidentes, incluindo testes regulares para garantir que elas estejam prontas para agir em caso de um incidente. Manter um plano atualizado de resposta a incidentes, que inclua os procedimentos necessários para minimizar o impacto nos negócios.

# Check (Verificar)

Monitorar e avaliar o processo implementado na etapa anterior.

* *EXEMPLO 1:* Monitorar regularmente a eficácia das medidas de segurança implementadas, por meio de auditorias de segurança e testes de penetração. Realizar revisões periódicas do SGSI para garantir que ele esteja alinhado com as mudanças na organização e no ambiente externo.
* *EXEMPLO 2:* Realizar testes regulares do plano de resposta a incidentes para garantir que ele ainda seja eficaz e atualizado. Avaliar o impacto dos incidentes que ocorreram para identificar oportunidades de melhoria.

# Act (Agir)

Agir com base nas avaliações realizadas na etapa anterior para melhorar continuamente o processo.

* *EXEMPLO 1:* Implementar as melhorias identificadas nas auditorias de segurança e revisões periódicas do SGSI. Continuar a alocar recursos suficientes para garantir a eficácia das medidas de segurança implementadas.
* EXEMPLO 2: Implementar as melhorias identificadas nos testes regulares do plano de resposta a incidentes. Continuar a atualizar o plano de resposta a incidentes com base nas avaliações realizadas e em novas ameaças ou vulnerabilidades identific