Experiência na Implantação do MR-MPS-SW Nível C e ABNT NBR ISO/IEC 27001 na Coopersystem

Edgard Amoroso[1], Marcela Calazans Medeiros Silva[1], Cristina Ângela Filipak Machado[2] e Renato Ferraz Machado[2]

[1]Coopersystem
Brasília – DF - Brasil

[2]Qualityfocus
Curitiba, PR - Brasil.

edgard.amoroso@coopersystem.com.br,marcela.calazans@coopersystem.com.br,
cristina.machado@qualityfocus.com.br, renato@qualityfocus.com.br

Abstract. *This article describes the implementation of MR-MPS-SW level C and ABNT NBR ISO/IEC 27001 at Coopersystem with the intersections between them, reuse of solutions, substantial differences found, and the strategies adopted during implementation. It also suggests future work that could be carried out in the organization to provide even greater integration.*

Resumo. *Este artigo descreve a implantação do MR-MPS-SW nível C e da ABNT NBR ISO/IEC 27001 na Coopersystem com as intersecções existentes entre elas, reuso de soluções, diferenças substanciais encontradas e as estratégias adotadas durante a implantação. Também sugere futuros trabalhos que poderão ser realizados na organização para proporcionar uma integração ainda maior.*

1. Introdução

No cenário atual de Tecnologia da Informação (TI), onde a segurança e a qualidade são imperativos, a certificação e/ou outro mecanismo de avaliação externa desempenha um papel crucial na construção da confiança dos clientes e na demonstração do compromisso de uma empresa com práticas sólidas. Duas, em especial, se destacam para uma empresa de TI: as avaliações providas pelo MPS.BR - Melhoria de Processo de Software e Serviços e a certificação ABNT NBR ISO/IEC 27001 - Sistemas de gestão da segurança da informação [ABNT 2013], chamada de ISO 27001.

A suas obtenções não são apenas o reconhecimento pela adoção de boas práticas corporativas, mas também oportunidades para melhorias contínuas. Elas estimulam uma cultura de inovação, aprendizado e adaptação, essenciais para enfrentar os desafios dinâmicos do setor de TI. Também permitem não apenas que a empresa se destaque no mercado, mas também produza alicerces sólidos para o crescimento sustentável. A busca pela excelência em processos e na segurança da informação não é apenas uma formalidade, mas uma jornada contínua em direção à entrega de soluções confiáveis e seguras em um mundo cada vez mais interconectado.

2. Implantação do MR-MPS-SW e ABNT NBR ISO/IEC 27001

A Coopersystem, focada no propósito de se destacar no mercado TI, obter novos clientes e segmentos de mercado, decidiu implementar em 2018 o MR-MPS-SW, começando pelo

nível “F” alcançado em 2021 e evoluindo para o nível “C” em 2022. Entre as suas pretensões, constava também a certificação ISO 27001, cujo trabalho iniciou-se em 2022 e a certificação aconteceu em julho de 2023.

Essas avaliações e certificações são importantes para alcançar os objetivos da Coopersystem e, em muitas situações, são exigidas em licitações, na apresentação de propostas junto a potenciais clientes ou na consolidação da manutenção dos atuais clientes.

3. Contribuição do MR-MPS-SW nível C para implantação da ABNT NBR ISO/IEC 27001

Os projetos de implantação do MR-MPS-SW Nível C e da ISO 27001 tiveram seu início em fevereiro e março de 2022, sucessivamente. A estratégia foi conduzir ambos os projetos de forma independente, com gerentes de projeto e cronogramas específicos, mas com alguns técnicos em comum para promover a integração e colaboração. Os escopos são diferentes, enquanto o MR-MPS-SW foca na área de desenvolvimento de software, a ISO 27001 foca na segurança da informação para toda a organização.

Como a Coopersystem tinha o nível F do MR-MPS-SW, muitos processos já existiam. Havia uma equipe dedicada a melhoria de processos e as ferramentas de apoio e de publicação da Arquitetura de Processos já estavam definidas. Isso fez com que o projeto da implantação do nível C fosse concluído com 7 meses, deixando a equipe de melhoria de processos dedicada ao apoio à implantação da ABNT NBR ISO/IEC 27001.

Desta forma, muitas das definições do MR-MPS-SW nível C foram de suma importância para a implantação da ISO 27001. A análise destas contribuições é o objeto deste artigo. Para tanto, iremos relacionar para cada requisito da ISO 27001 o que foi reusado da implantação do MR-MPS-SW. Também serão apresentados os controles do Anexo A, conforme Tabela 1. Os controles que não constam na Tabela 1 foram implementados exclusivamente para a ISO 27001.

Tabela 1- Cláusulas da ABNT NBR ISO/IEC 27001 e contribuição do MR-MPS-SW nível C

Cláusulas da 27001:2013	**Relacionamento com o MR-MPS-SW**
4. Contexto da organização	Foi descrito no Plano de SGSI o contexto da organização. Reutilizada a estrutura de melhoria do MR-MPS-SW
5 Liderança	O processo ORG foi reusado para garantir o alinhamento e comprometimento da liderança e para apoiar a Política de SI. O Processo MED foi utilizado para assegurar os resultados do SGSI. Os Processos ORG e GPC foram reusados com foco nas melhorias e alinhamento com o negócio.
6 Planejamento	O processo de RIS poderia ser utilizado, mas um processo específico foi criado complementando o relacionamento do risco com os controles do Anexo A, conceito de risco residual e a declaração de aplicabilidade. O planejamento para alcançar os objetivos de SI foi realizado como um projeto, reutilizando as ferramentas do MR-MPS-SW.
7 Apoio	O planejamento da implantação foi realizado conforme o MR-MPS-SW. As definições de recursos e da informação documentada (Arquitetura de Processos) foram reusadas do MR-MPS-SW (ferramentas e GCO). A classificação da informação foi implantada em todos os documentos.
8 Operação	As ferramentas e o processo de GCO foram reusados para os documentos do SGSI. Para mudanças nas ferramentas e ambientes foi criado o processo de Gestão de Mudanças.
9 Avaliação de desempenho	Reusado a definição da medição de MED para os indicadores de SI.

Cláusulas da 27001:2013	Relacionamento com o MR-MPS-SW
	O processo de GQA foi reescrito, juntamente com Checklists específicos. O acompanhamento do SGSI reutilizou a prática do MR-MPS-SW, mas como reunião específica para o SGSI pelo escopo ser mais abrangente.
10 Melhoria	A ferramenta foi reutilizada, mas foi configurada para que fossem analisadas as causas da não conformidade de forma individual.
A.6.1.5 SI no gerenciamento de projetos: Utilizado o processo de GPR na íntegra.	
A.7.2.1 Responsabilidades da Direção: Reutilizado os mecanismos de acompanhamento pela direção.	
A.7.2.2 Conscientização, educação e treinamento em SI: Reutilizado as mesmas ferramentas para treinamento, educação e conscientização do MR-MPS-SW.	
A.14.1.1 Análise e especificação dos requisitos SI: Adicionado ao processo de REQ os requisitos de SI.	
A.14.2.1 Política de desenvolvimento seguro: Criada política de desenvolvimento seguro complementando o processo de PCP.	
A.14.2.2 Procedimento para controle de mudanças de sistemas: Utilizado o processo de GCO.	
A.14.2.5 Princípios para projetar sistemas seguros: Utilizado o processo de PCP	
A.14.2.6 Ambiente seguro para desenvolvimento A.14.2.8 Teste de segurança do sistema A.14.2.9 Teste de aceitação de sistemas e A.14.3 Dados para teste: Reusados os Processos ITP e VV.	

4. Conclusões

Como a organização já tinha se submetido a avaliação MR-MPS-SW, algumas boas práticas trazidas do MR-MPS-SW e que não eram requisitos da ISO 27001, foram implantadas, tais como: arquitetura (inter-relacionamento, documentação e *templates* de processos, guias e documentos); gestão de configuração de processos; criação da planilha de avaliação para a ISO 27001, que serviu de apoio para a empresa durante a auditoria de certificação; ferramentas de repositório de processos, de qualidade e de gestão de melhoria do SGSI e cultura de definição de indicadores e de política organizacional.

Podemos concluir que a implantação do MR-MPS-SW foi um facilitador para o alcance dos objetivos da implantação da ISO 27001, pois parte da organização já tinha a cultura de processos, de auditoria de qualidade interna, levantamento de indicadores e acompanhamento da alta direção nas atividades de melhoria. Ademais, muitos colaboradores já haviam participado do processo de avaliação e se adaptaram com facilidade durante a certificação ISO 27001.

Foram ainda mapeadas questões a serem desenvolvidas de forma mais integrada visando o atendimento do MPS e ISO 27001: unificar o processo de gestão de riscos e oportunidades, unificar as políticas, auditorias de qualidade com os indicadores sendo coletados pela mesma equipe de forma a diminuir custos e recursos.

5. Referências Bibliográficas

[ABNT 2013], Tecnologia da informação — Técnicas de Segurança – Sistemas de gestão da segurança da informação — Requisitos, vol. ABNT NBR ISO/IEC 27001/2013. Associação Brasileira de Normas Técnicas, 2. Edição.

[SOFTEX 2023], MR-MPS-SW - Guia Geral MPS de Software, Disponível em: https://softex.br/download/guia-geral-mps-de-software2023/. Acessado em 29 de setembro de 2023.