1. OBJETIVO:

Estabelecer regras para a programação, realização de auditorias internas e para a tomada de ação corretiva, quando necessário.

2. ABRANGÊNCIA:

Esse procedimento abrange todos os documentos e atividades do Sistema de Gestão Segurança da Informação (SGSI) descritos no MSGSI - Manual do Sistema de Gestão de Segurança da Informação.

3. RESPONSABILIDADES:

3.1 Cabe ao elaborador digitar o documento, encaminhá-lo ao aprovador, distribuir cópias em papel se necessário, implementar, revisar e controlar este documento.

3.2 Cabe ao aprovador realizar a análise crítica deste documento, aprovando-o ou não para o uso.

3.3 RD = Revisar e avaliar a eficácia, suficiência e aplicação dos controles contábeis, financeiros e operacionais determinando o cumprimento das normas, dos planos e procedimentos vigentes, estabelecendo controle sobre os ativos da empresa e da sua proteção contra todo tipo de perda.

3.4 Alta Direção = Avaliar os riscos estratégicos e de negócio da organização.

3.5 Gestor do Processo = Avaliar a qualidade alcançada na execução de tarefas determinadas para o cumprimento das respectivas responsabilidades.

3.6 Colaboradores = compreensão mais amplas sobre as rotinas de outros departamentos e como estas rotinas se complementam para alcançar os resultados planejados e buscar uma maior compreensão dos resultados de seu trabalho e demais colaboradores.

4. DESCRIÇÃO:

4.1 O Representante da Direção (RD) é responsável pela programação das auditorias, com base na situação vigente, importância das atividades e áreas/elementos da norma (processos) a serem auditados e nos resultados das auditorias anteriores.

4.2 O Plano de auditoria compreende:

- Comunicação formal da auditoria;
- Áreas ou processos ou elementos da norma a serem auditados;
- Auditor designado e auditados;
- Período previsto (dia / mês / ano).

NOTA: No período de um ano, todos os processos deverão ser auditados obrigatoriamente pelo menos uma vez.

4.3 As auditorias podem ser conduzidas por colaboradores da ANTHEUS que não tenham vínculo direto com a área que está sendo auditada (evitando conflito de interesse).
Para conduzir as auditorias, os colaboradores devem apresentar as seguintes competências:

- Educação: segundo grau completo;
- Treinamento: participação em curso de formação de auditores internos;
- Experiência necessária: mínimo de 6 meses como colaborador da ANTHEUS;

4.4 A ANTHEUS pode fazer uso de profissionais externos contratados para a realização das auditorias internas.
Esses profissionais devem possuir certificação mínima no treinamento de auditor interno com apresentam evidências da realização de pelo menos 01 (uma) auditoria.

4.5 O R.D. coordena a realização das auditorias internas, com base na programa definida (item 4.1), cabendo ao auditor e ao auditado combinarem data e horário para a realização da auditoria, dentro do período estabelecido no Plano de Auditoria.

4.6 Os resultados da auditoria são registrados pelo auditor líder em Relatório de Auditoria Interna e as não conformidades nos Relatórios de Ação Corretivas (RACs). Cabe ao R.D. controlar a numeração dos RACs.

4.7 Se não houver nenhuma não-conformidade identificada ao longo da auditoria, o auditor líder exprime as conformidades no Relatório de Auditoria Interna. Em seguida, retém uma cópia do respectivo Relatório de Auditoria Interna e envia o original do mesmo ao RD, para este armazenar na pasta de Relatórios de Auditoria Interna.

4.8 Encontrada(s) não-conformidade(s), o auditor líder junto ao RD, faz a abertura das RACs, que serão encaminhadas ao responsável pelo processo auditado para a investigação da(s) causa(s) da não-conformidade(s) e planejar as ações necessárias.

4.9 Cabe ao responsável pela ação corretiva, registrar os resultados das ações executadas, e comunicar ao RD a data estimada para análise das ações para o encerramento das RACs.

4.10 O RD é responsável pela análise das ações corretivas executadas, preenchendo os campos reservados para analise nos RACs.

4.11 Se os resultados e as análises críticas das ações executadas indicarem a eliminação das causas da(s) não-conformidade(s), considera-se a ação corretiva eficaz. Caso contrário, o processo é reiniciado e definido novo prazo para a implantação das ações corretivas, mantendo-se o mesmo número do RAC.

4.12 As observações e oportunidades de melhoria descritas no Relatório de Auditoria Interna, serão registradas no Relatorio de Ação Preventiva (RAP), analisadas pela área auditada e pela área de SGI, que considerando pertinentes, poderão tratá-las (como não conformidade potencial).

5. REFÊRENCIAS:

- MSGSI - Manual do Sistema de Gestão de Segurança da Informação.

6. GLOSSÁRIO:

Ação Corretiva: É aquela que elimina a(s) causa(s) de uma não conformidade evitando a sua repetição.

Ação Preventiva: É aquela que previne a ocorrência de uma não conformidade potencial ou por abrangência previne falhas detectadas em outras áreas ou processos.

7. ANEXOS:

Não há.

8. REGISTROS:

- REG.9.2A - Plano de Auditoria Interna.
- REG.9.2B - Relatorio de Auditoria Interna.
- REG.9.2C - RAC - Relatorio de Ação Corretiva
- REG.9.2D - RAP - Relatorio de Ação Preventiva

9. PRAZO DE VALIDADE:

Este procedimento é válido a partir de sua emissão, devendo ser reavaliado anualmente a partir a data da última revisão.

10. HISTÓRICO DE MODIFICAÇÕES:

Revisão 0 em 03/05/2023: Elaboração Inicial.