1. OBJETIVO

Estabelecer a sistemática para avaliar a conformidade do sistema de gestão de segurança da informação com os requisitos da norma ABNT NBR ISO/IEC 27001.

2. ABRANGÊNCIA

Este procedimento aplica-se aos processos que fazem parte do escopo do SGSI.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos
- Norma ABNT NBR ISO 19011 – Diretrizes para Auditoria de Sistema de Gestão

4. DEFINIÇÕES

- Auditoria**:** é um processo sistemático e documentado de obtenção de evidência objetiva, para avaliar se os critérios de auditoria foram atendidos.
  Obs.: A auditoria interna pode ser conduzida por auditor interno do NEES ou por terceiros, contratados para esta finalidade.
- Auditor**:** Pessoa com competência para realizar a auditoria.
- Auditor **Líder:** É um auditor designado para gerenciar uma equipe de auditoria.
- Auditado**:** Organização que está sendo auditada.
- Evidência **de Auditoria:** Registros, apresentação de fatos ou outras informações pertinentes aos critérios de auditorias e verificáveis.
  Nota: Evidência de auditoria pode ser qualitativa ou quantitativa.
- Não **Conformidade:** Não atendimento a um requisito.
- Programa **de Auditoria:** é o planejamento de uma ou mais auditorias, para um período e direcionado a um propósito específico.
- Plano **de Auditoria:** Descrição das atividades e arranjos para uma auditoria.

Elaborador: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-04-28 16:40
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-04-28 17:13
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-04-29 10:41

5. DIRETRIZES

5.1 Etapas da Auditoria

5.1.1 Programação da Auditoria Interna

O Gestor do SGSI é responsável por definir a Programação de Auditoria, assegurando que a integridade da auditoria seja mantida.

O programa de auditoria deve abordar os requisitos da norma ISO/IEC 27001 e incluir as seguintes informações:, deve ser registrado no FP017 - Programa de Auditoria Interna.

- Objetivo do Planejamento: Alinhar o planejamento das auditorias internas da organização.
- Duração da Auditoria: Informar qual será a duração das auditorias (dias).
- Escopo da Auditoria: Informar a abrangência da auditoria em relação aos requisitos e as normas a serem auditadas.

NOTA: O escopo da auditoria deve ser realizado de forma que dentro de um ano todos os requisitos do sistema de Gestão de segurança da informação sejam auditados.

- Periodicidade: Planejar o(s) mês(es) em que a auditoria será realizada.
- Frequência: informar a frequência em que as auditorias são realizadas, quantas vezes por ano.
- Tipo de Auditoria: Auditoria remota.
- Auditores: informar o nome do auditor líder e dos auditores que irão compor a equipe, quando for o caso.
- Processos: Informar os processos a serem auditados.
- Responsáveis: informar o nome dos responsáveis pelo(s) processo(s) a ser auditado (pessoa a ser auditada).
- Data de emissão do planejamento.
- Assinatura do elaborador

Encaminhar a Programação da Auditoria Interna por e-mail, com no mínimo 30 dias de antecedência, para Diretoria Executiva e Lideranças, com o objetivo de divulgar e preparar as equipes a serem auditadas. Realizar reunião, se necessário, com as lideranças.

5.2 Execução da Auditoria

5.2.1 Reunião de Abertura

O Auditor Líder deve se apresentar e apresentar a equipe de auditores, quando for o caso. Estabelecer as regras básicas para a auditoria, confirmar a Programação da Auditoria, tais como:

- Confirmar o escopo e objetivos da auditoria;
- Explicar a metodologia;
- Confirmar a disponibilidade de recursos;
- Compartilhar as informações sobre a auditoria;
- Apresentar os objetivos preliminares;
- Apresentar o que se espera da gestão.

Devem estar presentes a Direção e/ou pessoa designada por esta, lideranças e responsáveis pelos processos.
Registrar a reunião de abertura em Ata de Reunião.

5.2.2 Análise de Evidências

Auditor deve analisar as evidências de auditoria interna, sendo informações coletadas para sustentar suas conclusões. As evidências podem ser obtidas em forma de documentos, registros, observações, confirmações, entre outros:
Verificar o tratamento das não conformidades da auditoria anterior, se existem pendências, avaliar a necessidade de abrir uma nova não conformidade.
Registrar a(s) conformidade(s), não conformidade(s) e observação(ões) de melhoria, incluindo a rastreabilidade necessária, de forma que sejam de fácil entendimento.
Comunicar ao auditado, no momento da auditoria, caso identifique não conformidade.

5.2.3 Reunião Encerramento

O Auditor Líder deve agradecer a participação de todos e apresentar o resultado da auditoria. Devem ser discutidas as conformidades do sistema, as não conformidades e as oportunidades de melhoria. Perguntar se a equipe tem alguma dúvida e encerrar a auditoria interna.

5.2.4 Relatório de Auditoria Interna

O auditor líder deve elaborar o relatório da auditoria interna, incluindo o resultado.
Relatar o desempenho atual da organização, descrever as não conformidades e observações de melhoria, caso sejam identificadas.
Disponibilizar o relatório para o(a) Responsável SGI para que seja divulgado internamente, e tomadas as providências, quando necessário.

5.3 Responsabilidades / Autoridades

5.3.1 Direção

- Participar e estimular a autorizar a participação da equipe na auditoria interna;
- Disponibilizar recursos para as tratativas das não conformidades;
- Apoiar a implantação das melhorias, quando pertinentes.

5.3.2 Responsável SGI:

- Planejar as auditorias.
- Comunicar o programa de auditoria as partes interessadas internas.
- Coordenar e programar auditorias e outras atividades pertinentes ao programa de auditoria.
- Estabelecer e manter um processo para avaliação dos auditores e seu desenvolvimento profissional contínuo.
- Escolher o auditor líder e a equipe de auditoria assegurando a competência da auditoria e da equipe.
- Solicitar recursos necessários para as equipes de auditorias.
- Manter registros do programa de auditoria.
- Assegurar a análise crítica e a aprovação de relatórios de auditoria e assegurar sua distribuição ao cliente da auditoria e outras partes específicas.
- Monitorar o desempenho e eficácia do programa de auditoria.
- Informar para a Direção o resultado das auditorias.

5.3.3 Auditor Líder e equipe de Auditores

- Realizar auditoria de acordo com a programação aprovada.

5.3.4 Bolsistas

- Participar das reuniões de auditoria.
- Emitir ações preventivas, oportunidades de melhoria e ações corretivas, quando necessário.
- Realizar a análise das causas das não conformidades.
- Programar e analisar o andamento das ações.

5.4 Revisão e Atualização

- Este procedimento deve ser revisto e atualizado anualmente.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Programa de Auditoria
- Relatório de Auditoria

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Procedimentos. Deve ser atualizado anualmente.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	30/01/2025	Criação do documento.	Shirley Vital
02	15/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital