# Propósito

A Norma de Auditoria Interna **NOR-SGSI-014** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para a manutenção e execução anual de auditorias internas com objetivo de verificar a conformidade com requisitos da **Demarco** para seu SGSI e SGP (baseados na ISO/IEC 27.001 e na ISO/IEC 27.701).

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação e Política de Proteção de Dados.

# Glossário

**Ação corretiva:** Ação para eliminar a causa de uma não conformidade identificada ou outra situação indesejável existente, a fim de prevenir sua repetição.

* **Ação imediata:** primeira ação feita quando uma não conformidade é percebida na empresa. Essa ação é feita para controlar a ocorrência, impedindo que ela continue acontecendo no momento, e é realizada após a identificação do problema.
* **Ação preventiva:** ação feita antes da não conformidade acontecer. Pode ser um evento inédito na empresa, ou inédito em um processo. Portanto, **são analisados os riscos que foram previamente detectados sobre uma potencial não conformidade** e assim é definida a ação que impedirá essa ocorrência.
* **Auditado:** Organização, área ou pessoa que está sendo avaliada.
* **Auditor:** Pessoa que realiza uma auditoria.
* **Auditor Líder:** Pessoa designada para conduzir a equipe de auditoria.

**Auditoria:** Processo sistemático, documentado e independente para obter evidência objetiva e avaliá-las para determinar a extensão na qual os critérios de auditoria são atendidos.

**Conformidade:** Atendimento a requisitos de Segurança da Informação ou Privacidade.

**Competência:** Capacidade de aplicar conhecimentos e habilidades para atingir resultados pretendidos na execução da auditoria.

* **Constatações da Auditoria:** Resultados da avaliação da evidência de auditoria coletada, comparada com os critérios de auditoria.

* **Critério de auditoria**: Conjunto de políticas, procedimentos ou requisitos usados como uma referência na qual a evidência de auditoria é comparada.
* **Escopo da auditoria:** Abrangência e limites de uma auditoria.
* **Evidência de Auditoria:** Registros, apresentação de fatos ou outras informações pertinentes aos critérios de auditoria e verificáveis.
* **Não conformidade:** Não atendimento a um requisito de Segurança da Informação ou Privacidade
* **Risco:** Possibilidade de ocorrência de um evento que possa impactar, positiva ou negativamente, a implementação das estratégias ou a realização dos objetivos da organização, sendo mensurado em termos de impacto e de probabilidade.

Diretrizes

Para assegurar que os requisitos de Segurança da Informação e Privacidade estão em conformidade, deve ser estabelecido e mantido programa de auditoria interna. As seguintes diretrizes devem ser observadas:

## Programa de auditoria

Deve ser estabelecido um programa anual de auditoria, considerando a abrangência do programa e a frequência de auditorias;

1. No mínimo, deve ser realizada 1 (uma) auditoria interna por ano;
2. Deve ser realizada avaliação para determinar os recursos necessários para a realização das auditorias internas;

O programa de auditoria interna deve ser monitorado, analisado e melhorado continuamente;

O programa de auditoria deve levar em consideração os requisitos legais aplicáveis aos processos da **Demarco.**

## Princípios da auditoria e Atributos pessoais dos auditores

Os auditores devem atuar de acordo com os seguintes princípios e possuir atributos pessoais associados a eles:

1. Princípio de conduta ética, que é o fundamento do profissionalismo. Os atributos associados estão em ser ético, confiável, íntegro.
2. Princípio de apresentação justa, que é a obrigação de reportar com veracidade e exatidão. Os atributos associados estão em ser observador, estando ativamente atento aos arredores e às atividades ser tenaz, persistente e focado em alcançar os objetivos;

Princípio do cuidado profissional, que é a aplicação de diligências e julgamento na auditoria. Os atributos associados estão em ter flexibilidade e escuta ativa, atuar com diplomacia, tato e empatia ao lidar com as pessoas;

1. Princípio de independência, que é a base para a imparcialidade da auditoria e objetividade das conclusões. Os atributos associados estão em ser decisivo e chegar a conclusões oportunas, baseadas em evidências.;
2. Princípio de abordagem baseada em evidência, que é o método racional para alcançar conclusões de avaliações confiáveis e reproduzíveis em um processo sistemático de Auditoria.

(juntar com V) Os atributos associados estão em ser versátil ao ajustar-se prontamente a diferentes situações, podendo a abordagem ser baseada em amostras de informações disponíveis, uma vez que a auditoria é feita em período limitado e com recursos finitos.

## Conhecimentos e Habilidades dos auditores

Os auditores devem ter conhecimentos e habilidades comprovadas nas seguintes áreas:

1. Princípios, normas e técnicas de auditoria, em particular a ISO 19011:2019;
2. Sistema de Gestão de Segurança da Informação, baseado na ISO/IEC 27.001:2022;

Sistema de Gestão de Privacidade, baseado na ISO/IEC 27.701:2019;

Políticas, normas e procedimentos da área a ser auditada, incluindo o escopo e os critérios de auditoria ;

## Leis, regulamentos e outros requisitos pertinentes à disciplina aplicável. Planejamento da Auditoria

1. O Comitê de Segurança da Informação e Privacidade deverá entrar em contato com o(s) colaborador(es) indicado(s) para as entrevistas de auditoria interna para combinar a data da auditoria e qual documentação será verificada.

O Comitê de Segurança da Informação e Privacidade deverá disponibilizar aos auditores, através de compartilhamento seguro de pastas, a documentação do SGSI e SGP para avaliação.

Os auditores devem estudar as normas e documentos do SGSI e SGP, ler o relatório da última auditoria e preparar o plano de auditoria.

## Execução da Auditoria

A auditoria interna deve no mínimo considerar três etapas:

1. **Reunião de Abertura:** Deve ter como objetivo:

* Apresentar os auditores e os participantes que representarão a empresa na auditoria;
* Confirmar os pontos que serão auditados;
* Discutir sobre as referências normativas a serem utilizadas;
* Os princípios e premissas para a auditoria;
* Elencar os tipos de constatações da auditoria;
* Entregas a serem realizadas.

**Realização da Auditoria:** Deve ser realizada através de:

* Uma lista de verificação apresentada pelos auditores;

Os auditores devem se certificar de que tudo seja documentado de modo claro, conciso e comprovado por evidência;;

* Deve ser feita através de análises das evidências encontradas, seja através de entrevistas, exames de documentos e observação de atividades ou condições das áreas auditadas;
* As informações obtidas por meio de entrevistas devem ser comprovadas com outras fontes independentes, tais como medições e registros;
* Caso existirem não conformidades, estas devem ser anotadas e relatadas no momento para o colaborador entrevistado;

Todas as observações e indícios de não conformidade identificados durante a auditoria devem ser anotados. Concluída as atividades de auditoria, os auditores devem analisá-las para determinar se serão registradas como não conformidades;

As não conformidades devem ser identificadas de acordo com os requisitos específicos da organização e aos documentos apresentados, a partir dos quais a auditoria foi realizada;

**Reunião de encerramento:** Para a conclusão da auditoria, deve ser feito:

* Uma reunião junto aos auditores e participantes da auditoria;
* Apresentação executiva dos resultados da auditoria, que considere as observações relevantes, não conformidades identificadas, oportunidades de melhorias, pontos positivos identificados durante a auditoria e conclusão dos auditores sobre o SGSI e a estrutura de privacidade da empresa.

## Registros de auditoria

Devem ser mantidos como registros de auditoria:

* Programação anual de auditoria;
* Documentação e pauta de reuniões de abertura;
* Documentação e pauta da reunião de encerramento;
* Certificado que comprove competências do(s) auditor(es);
* Relatórios de auditoria interna.

# Papéis e Responsabilidades

## PRESIDÊNCIA

1. Aprovar proposta de auditoria interna;

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Estabelecer e manter atualizada a programação anual de auditorias;
2. Avaliar e determinar quais são os recursos necessários para a programação anual de auditoria;
3. Avaliar, quando necessário, propostas de diferentes empresas para a realização de auditoria interna;
4. Indicar os colaboradores ou membros do CSIP para representar as áreas a serem auditadas;
5. Comunicar as datas da auditoria aos gestores das áreas a serem auditadas, com uma antecedência de 15 (quinze) dias;
6. Conduzir ou solicitar as auditorias de follow up, referentes às ações corretivas e melhorias propostas, monitorando os prazos estabelecidos e registrando as evidências objetivas, com vistas ao seu fechamento;
7. Promover a rotatividade da equipe de auditores, durante o ciclo das auditorias internas;
8. Reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria;
9. Estabelecer planos de ações imediatas, corretivas e melhorias; monitorar os prazos estabelecidos, registrando as evidências objetivas para a conclusão das ações imediatas e corretivas;

## AUDITOR LÍDER

1. Elaborar o plano de auditoria interna do Sistema de Gestão de Segurança da Informação, considerando a situação e importância dos processos e das áreas a serem auditadas, bem como os resultados de auditorias anteriores;
2. Assegurar que todos os requisitos da organização, da norma ISO/IEC 27.001 pertinentes e sejam contemplados no plano da auditoria;
3. Conduzir a reunião inicial, definindo o planejamento da auditoria e as atividades de cada auditor;
4. Executar o plano da auditoria interna;
5. Coordenar todas as fases da auditoria interna;
6. Manter-se dentro do escopo da auditoria;
7. Conduzir a reunião de encerramento;
8. Elaborar o relatório de auditoria interna, incluindo o propósito, programa e resultados da auditoria, assim como a identificação de aspectos positivos e oportunidades para melhoria;
9. Registrar as não conformidades identificadas na auditoria interna;
10. Assegurar que os resultados das auditorias são relatados para a Presidência da **Demarco**, representada pelo Comitê de Segurança da Informação e Privacidade;

## GESTOR DE ÁREA

1. Informar aos colaboradores de sua área os objetivos e o escopo da auditoria;
2. Prover o acesso às instalações e ao material comprobatório, conforme solicitado pelos auditores;
3. Cooperar com os auditores para permitir que os objetivos da auditoria interna sejam atingidos;
4. Preencher o formulário de “Avaliação de Desempenho da Equipe de Auditoria” e encaminhá-lo ao Comitê Gestor de Segurança da Informação.

# Gestão de versões

A revisão, aprovação e alteração desta norma segue os requisitos estabelecidos na Política de Segurança da Informação.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 04/09/2023 | CSIP | Criação |
| 0.2 | 10/07/2024 | CSIP | Revisão anual |
|  |  |  |  |