Documento analisado criticamente e aprovado quanto à sua adequação.	Responsáveis: Adriana Silva de Assis Oliveira – Diretora Técnica Carlos Henrique R. Figueiredo – Diretor de Certificação

ÚLTIMAS ALTERAÇÕES	
Data:	**Revisão:**
25/11/2025	Emissão inicial

1 - Objetivo

A presente Publicação 16 ou Regulamento Geral da Certificação de Sistemas de Gestão de Segurança da Informação (Pb16), complementando o disposto no Manual de segurança da informação da SAS CERTIFICADORA Ltda. estabelece requisitos: da certificação de Sistemas de Gestão de Segurança da Informação; da concessão, uso e cancelamento do respectivo Certificado de Sistemas de Gestão de Segurança da Informação SAS; e outros correlatos e/ou afins.

1.1 - O Certificado de Sistemas de Gestão de Segurança da Informação SAS é um certificado de conformidade com a norma brasileira:

NBR ISO/IEC 27001:2022 - Sistemas de Gestão de Segurança da informação— Requisitos

1.2 - A concessão do Certificado de Sistemas de Gestão de Segurança da Informação SAS implica na avaliação e controle das condições particulares do Sistema de Gestão de segurança da informação para determinada atividade coberta pelo escopo da organização, mas não constitui uma certificação de produtos, processos ou serviços.

2 - Solicitação de Certificação de Sistemas de Gestão de Segurança da informação SAS

2.1 - A SAS exige que um representante autorizado da organização solicitante forneça as informações necessárias para lhe permitir estabelecer o seguinte:

a) o escopo desejado da certificação;
b) detalhes pertinentes da organização solicitante conforme requerido pelo esquema de certificação específico, incluindo seu nome e o endereço das suas plantas, seus processos e operações, recursos técnicos e humanos, funções, relacionamentos e quaisquer obrigações legais pertinentes;
c) identificação de todos os processos terceirizados usados pela organização que afetarão a conformidade com os requisitos;
d) as normas ou outros requisitos para os quais a organização solicitante busca certificação;
e) se consultoria relativa ao sistema de gestão de segurança da informação a ser certificado foi fornecida e, se sim, quem forneceu.

NOTAS:
1 - Para sistemas de gestão integrados, deve incluir informações relativas ao nível de integração, incluindo o nível de integração de documentos, elementos do sistema de gestão e responsabilidades.
2 - Para transferência de certificação, deve incluir o motivo que levou à transferência para a SAS (caso não informe o motivo, esta opção deve ser formalizada).

2.2 - Para a solicitação será utilizado o formulário Questionário de Avaliação Preliminar - FORM. 7. fornecido pela SAS, que inclui:

Informações do cliente relacionadas ao número de pessoas que executam certas atividades idênticas, incluindo:

— O número de pessoas que exercem a atividade;
— o tipo de atividade ou processo.

Exemplos de fatores que podem reduzir o número de pessoas usadas como base de cálculo que estão realizando certas atividades idênticas incluem:

— pessoas com acesso somente leitura à informação para desempenhar suas funções;
— pessoas sem acesso às instalações de processamento de informações da organização no âmbito do SGSI;
— pessoas que têm acesso restrito demonstrável específico às instalações de processamento de informações da empresa no escopo do SGSI;
— pessoas que exercem atividades em que são implementadas limitações estritas para restringir a divulgação de informações, por exemplo, medidas que proíbem pertences e dispositivos pessoais na área de trabalho.

NOTAS:
1 - Para sistemas de gestão integrados, deve incluir informações relativas ao nível de integração, incluindo o nível de integração de documentos, elementos do sistema de gestão e responsabilidades.
2 - Para transferência de certificação, deve incluir o motivo que levou à transferência para a SAS (caso não informe o motivo, esta opção deve ser formalizada).

3 - Análise da Solicitação

3.1 - Recebendo o Questionário de Avaliação Preliminar devidamente respondido, a SAS procederá uma análise crítica da solicitação e das informações suplementares de certificação para assegurar que:

a) As informações sobre a organização solicitante e seu Sistema de Gestão de Segurança da Informação sejam suficientes para desenvolver um programa de auditoria, para a emissão da Proposta técnica-comercial/Contrato e para realização da auditoria;

b) Qualquer diferença reconhecida de interpretação entre a SAS e a organização solicitante seja resolvida;

c) A SAS tenha competência e capacidade para executar a atividade de certificação;

d) O escopo solicitado para a certificação, a(s) planta(s) das operações da organização solicitante, o tempo necessário para completar as auditorias e quaisquer outros pontos que influenciem o serviço de certificação sejam levados em consideração (idioma, condições de segurança, ameaças à imparcialidade etc.);

A SAS utilizará os seguintes formulários e modelos, bem como os documentos abaixo aplicáveis:

- FORM. 7 - Questionário de Avaliação Preliminar;
- FORM. 9.1 – Proposta técnica-comercial / Contrato de Certificação SAS - Sistemas de Gestão;
- Registros de competências dos auditores e técnicos especialistas.

NOTA:
Deve ser conferida a compatibilidade da atividade econômica principal da organização constante do CNPJ – Cadastro Nacional de Pessoa Jurídica e escopos de certificação solicitados.

3.2 - Após a análise crítica da solicitação, a SAS aceita ou recusa a solicitação para a certificação. O aceite é evidenciado através do encaminhamento por e-mail ao solicitante do FORM. 9.1 – Proposta técnica-comercial / Contrato de Certificação SAS - Sistemas de Gestão. Quando a SAS recusa uma solicitação para certificação como resultado da análise crítica, ela documenta os motivos para a recusa da solicitação e deixa claro para o cliente.

3.3 - Com base nesta análise crítica, a SAS determina as competências adequadas que serão necessárias para incluir em sua equipe auditora e para a decisão da certificação.

4 - Aceite da Proposta técnica-comercial/Contrato de Certificação SAS e envio de documentos complementares

4.1 - Estando de acordo com a Proposta técnica-comercial/Contrato de Certificação SAS, a organização solicitante deverá formalizar o seu aceite, encaminhando por e-mail a SAS, o FORM. 9.1 – Proposta técnica-comercial / Contrato de Certificação SAS - Sistemas de Gestão com assinatura na última página e rubrica nas demais, juntamente com a documentação abaixo, para confirmação do agendamento das auditorias:
- Cópia do Contrato Social e alterações contratuais ou última alteração consolidada e seu registro na Junta Comercial ou órgão equivalente; ou Estatuto da organização.

4.2 - Em caso de alteração dessa documentação, a mesma deverá ser encaminhada a SAS sob o risco de perda da concessão ou manutenção da certificação e poderá ser solicitada à organização pelo auditor líder para análise, quando da realização da auditoria de supervisão, conforme FORM. 8 – Lista de documentos da empresa solicitante.

5 - Programa de auditoria

5.1 - Um programa de auditoria - FORM. 10, para o ciclo completo de certificação, de três anos, é elaborado pela SAS, sob a supervisão da Diretoria de Certificação e/ou Técnica para identificar claramente a(s) atividade(s) de auditoria necessária(s) para demonstrar que o sistema de gestão de segurança da informação do cliente atende aos requisitos para certificação para a(s) norma(s) selecionada(s) ou outro(s) documento(s) normativo(s). O programa de auditoria para o ciclo de certificação cobre todos os requisitos do sistema de gestão de segurança da informação.

5.2 - O programa de auditoria inclui uma auditoria inicial em duas fases, auditorias de supervisão (manutenção) no primeiro e no segundo ano após a decisão de certificação, e uma auditoria de recertificação no terceiro ano, antes do vencimento da certificação. O primeiro ciclo de certificação de três anos inicia-se com a decisão de certificação. Os ciclos subsequentes iniciam com a decisão de recertificação. A determinação do programa de auditoria e de quaisquer ajustes subsequentes considera o tamanho da organização cliente, o escopo e a complexidade de seu sistema de gestão, produtos e processos, assim como o nível demonstrado de eficácia dos Sistemas de Gestão de Segurança da Informação e os resultados de quaisquer auditorias anteriores.

5.2.1 – As auditorias de supervisão deverão ser realizadas no mínimo uma vez a cada ano do calendário, exceto em anos de recertificação. A data da primeira auditoria de supervisão, após a certificação inicial, não pode ultrapassar 12 meses a partir da data da decisão da certificação (ver 14.2.2).

5.3 - Em casos em que a organização e/ou a SAS é afetada por algum evento fora de seu controle ou evento de força maior, ou em outros casos, a critério da SAS, é analisada a viabilidade, riscos e oportunidades, podendo:
- Realizar uma auditoria presencial conforme previamente programado;
- Optar por realizar uma auditoria remota parcial e posteriormente uma auditoria presencial complementando os requisitos mínimos necessários (quando a visita à obra for imprescindível, por exemplo);
- Realizar uma auditoria totalmente remota (em caso de ausência de obras, por exemplo);
- Recomendar postergar a realização da auditoria completa presencial e/ou
- Estender a validade do certificado sem a realização de auditoria por, no máximo, 6 (seis) meses, na qual serão então avaliados todos os requisitos previstos no programa de auditoria. Neste caso, não haverá alteração no ciclo da certificação, mantendo-se, mesmo em caso de recertificação, a data prevista para a próxima auditoria (sempre que possível).

5.3.1 - São analisadas as respostas da organização às questões de evento de força maior, que são encaminhadas previamente pela SAS por e-mail, e outros requisitos necessários para garantir um resultado de auditoria eficaz, levando em consideração, a maneira como a organização estará operando no momento do evento, o uso de equipamentos e o tipo e a complexidade da organização (atividades/serviços administrativos ou atividades de construção, industriais, saúde, mineração, agronegócio, transporte e outros).

NOTA:
São considerados eventos fora de seu controle ou evento de força maior: guerras, greves, instabilidade política, tensão geopolítica, terrorismo, crime, pandemia, terremoto, inundação, invasão criminosa de computadores ou outros desastres naturais ou causados pelo homem.

5.4 - Pode ser necessário também, ajustar a frequência das auditorias de supervisão para acomodar fatores como sazonalidade, eventos de força maior ou certificação de sistemas de gestão de duração limitada (ex. plantas de construção temporárias), podendo haver também ajustes no dimensionamento do tempo total de auditoria.

5.5 - Quando a SAS levar em conta certificação já concedida ao cliente e auditorias realizadas por outro organismo de certificação, ele obtém e mantém evidências suficientes, como relatórios e documentação de ações corretivas para qualquer não conformidade (ver item 13.4).
A SAS, baseada na informação obtida, justifica e registra quaisquer ajustes ao programa de auditoria existente e acompanha a implementação de ações corretivas relativas a não conformidades anteriores.

5.6 - Onde o cliente opera em regime de turnos, as atividades que acontecem durante o turno de trabalho devem ser consideradas na elaboração do programa de auditoria e nos planos de auditoria.

5.7 Considerações gerais

O programa de auditoria para auditorias SGSI leva em consideração os controles de segurança da informação determinados pelo cliente.

NOTA 1: Os controles de segurança da informação podem ser da NBR ISO/IEC 27001:2022, Anexo A e/ou outra(s) norma(s) aplicável(is) e/ou autoprojetados.

NOTA 2: Mais orientações sobre auditoria são fornecidas na ISO/IEC 27007.

6 - Determinação do tempo de auditoria

6.1 - O procedimento documentado da SAS para determinar o tempo de auditoria está descrito no Anexo C desta Pb, e para cada cliente é calculado o tempo necessário para planejar, realizar e relatar uma auditoria completa e eficaz do sistema de gestão de segurança da informação do cliente.

6.2 - Ao determinar o tempo de auditoria, a SAS considera, entre outros, os seguintes aspectos:

a) os requisitos da norma de sistema de gestão pertinente;

b) complexidade do cliente e seu sistema de gestão de segurança da informação;

c) contexto tecnológico e regulatório;

d) qualquer terceirização de quaisquer atividades incluídas no escopo do sistema de gestão de segurança da informação;

e) os resultados de quaisquer auditorias anteriores;

f) o tamanho e o número de locais, sua localização geográfica e considerações de *multi-site*;

g) os riscos associados aos produtos, processos ou atividades da organização;

h) se as auditorias são combinadas, conjuntas ou integradas.

NOTAS:
1 - O tempo gasto em deslocamento para chegar e deixar os locais auditados não está incluído no cálculo da duração da auditoria do sistema de gestão.

2 - Em caso de auditoria, remota, a determinação do tempo de auditoria não leva em consideração possíveis falhas de conexão. Caso essas falhas ocorram, deverão ser avaliadas pelo auditor líder, que deverá fazer os ajustes necessários no plano de auditoria juntamente com a organização auditada. Em casos de dúvidas ou impossibilidade de se prosseguir com a auditoria, a SAS deverá ser contatada pelo auditor líder.

6.3 - A duração da auditoria do sistema de gestão e a sua justificativa são registrados através do software de gerenciamento de auditorias SAS, com auxílio das informações constantes no Questionário de Avaliação Preliminar - FORM. 7 e nos Dados das Obras e Dados Complementares – FORM. 7.2.

6.4 - O tempo utilizado por qualquer membro da equipe que não for designado como auditor (por exemplo, especialistas técnicos, tradutores, intérpretes, observadores e auditores em treinamento) não contam na duração da auditoria de sistema de gestão estabelecida.

NOTAS:
1 - Para o uso de tradutores e intérpretes pode ser preciso um tempo adicional de auditoria.

2 - Para o uso de TICs (tecnologias de informação e comunicação) pode ser preciso tempo adicional bem como pode haver redução do tempo e eventual ganho de amostragem, conforme avaliação da SAS.

6.5 - A SAS Certificadora utiliza o Anexo C para determinar o dimensionamento da auditoria.

7 - Observadores, especialistas técnicos e guias

7.1 - Observadores

A presença e a justificativa para observadores durante uma atividade de auditoria são acordadas entre a SAS e o cliente antes da realização da auditoria. A equipe auditora assegura que os observadores não influenciem ou interfiram indevidamente no processo ou no resultado da auditoria.

NOTA:
Os observadores podem ser membros da organização do cliente, consultores, pessoal do organismo de acreditação realizando uma testemunha, reguladores ou outras pessoas justificadas.

7.2 - Especialistas técnicos

O papel dos especialistas técnicos durante uma auditoria é acordado entre a SAS e o cliente antes da condução da auditoria. Um especialista técnico não atua como auditor na equipe auditora. Os especialistas técnicos são acompanhados por um auditor.

NOTA:
Os especialistas técnicos podem fornecer assessoramento à equipe auditora para a preparação, planejamento ou auditoria.

7.3 - Guias

Cada auditor será acompanhado por um guia, a menos se acordado de outra forma pelo auditor líder e pelo cliente. Os guias são designados pela equipe auditora para facilitar a auditoria. A equipe auditora deve assegurar que os guias não influenciem ou interfiram no processo ou no resultado da auditoria, podendo solicitar sua substituição, quando apropriado.

NOTAS:
1 - As responsabilidades de um guia podem incluir:

a) estabelecer contatos e horários para entrevistas;

b) organizar visitas para partes específicas do local ou da organização;

c) assegurar que regras relativas aos procedimentos de segurança e seguridade do local sejam conhecidas e respeitadas pelos membros da equipe auditora;
d) testemunhar a auditoria em nome do cliente;

e) fornecer esclarecimento ou informações, conforme requisitado pelo auditor.

2 - Quando apropriado, o auditado pode também atuar como guia.

8 – Plano de auditoria

8.1 - Generalidades

8.1.1 - A SAS assegura, através do FORM. 11 - Carta de Comunicação de Auditoria, que um plano de auditoria é estabelecido antes de cada auditoria identificada no programa de auditoria, que sirva de base para um acordo em relação à realização e programação das atividades de auditoria.

8.1.2 - O plano de auditoria é elaborado pela SAS, sob a supervisão da Diretoria de Certificação e/ou Técnica. Sempre que necessário, o auditor líder também elaborará o plano de auditoria ou revisará o planejamento durante a auditoria.

8.1.3 - Nos casos em que a organização certificada e/ou a SAS é afetada por algum evento fora de seu controle ou de força maior que não permita a realização no prazo previsto das auditorias programadas, a SAS planeja suas ações:

- Contatando os clientes individualmente ou através de carta circular e/ou inserindo informações no website;
- Avaliando, caso a caso, se os procedimentos SAS permitem que o evento previsto pode ser postergado e eventuais ações necessárias e riscos decorrentes deste adiamento (auditoria remota ou documental para análise de risco de adiamento ou extensão da validade do certificado);
- avaliando a necessidade, a possibilidade e os riscos e oportunidades de realizar a auditoria total ou parcialmente de forma remota com utilização de Tecnologia da Informação e Comunicação – TIC;
- provendo os devidos treinamentos de forma a garantir que as ações tomadas sejam eficazes e garantam que as decisões decorrentes sejam baseadas em evidências objetivas.

8.1.4 - A SAS avalia a complexidade da organização e tipo de auditoria apropriados. No caso de organizações, processos ou produtos e serviços complexos e onde os objetivos do tipo de auditoria exigem uma avaliação completa da amostra padrão e mais ampla, uma análise cuidadosa da viabilidade das auditorias remotas para avaliar completamente a conformidade da organização todos os requisitos devem ser executados.

8.1.5 - A SAS se baseia na identificação documentada dos riscos e oportunidades que podem impactar a auditoria, para decisão de realização das auditorias com utilização de TICs.

NOTA: O plano de auditoria faz referência às ferramentas tecnológicas usadas para auxiliar a auditoria remota.

8.1.6 - Decisão pela realização de auditoria remota

8.1.6.1 - A conclusão sobre a decisão de se realizar ou não a auditoria remota cabe a SAS Certificadora e é baseada na avaliação da infraestrutura apropriada, no tipo de auditoria, na complexidade dos processos e na capacidade de atender aos objetivos da auditoria.

8.1.6.2 - Todas as outras situações potenciais devem ser tratadas por medidas apropriadas a serem refletidas conforme necessário no plano de auditoria. Apesar de usar métodos de auditoria remota, a confiança de que os objetivos de auditoria desejados serão alcançados deve ser mantida.

8.1.6.3 - Todas as análises de risco e oportunidades, bem como a decisão da SAS, são registradas e comunicadas às organizações certificadas.

8.1.7 - Para a realização de auditorias remotas é utilizada TIC – Tecnologia da Informação e Comunicação, preferencialmente através da ferramenta “Microsoft Teams" ou similar autorizado pela SAS (link a ser informado pela SAS). A equipe auditora e a organização devem prover de equipamento apropriado para realização da auditoria, tais como notebook com tela de no mínimo 10 polegadas, câmera própria ou externa e microfone, para que seja permitida a perfeita visualização e comunicação com a organização cliente.

O uso de aparelho celular também é permitido, mas deve ser utilizado apenas quando não tiver outra opção, em caso de perda de comunicação total durante a auditoria através da ferramentas TIC – Tecnologia da Informação e Comunicação ou similar no notebook. O uso de aparelho celular também é permitido, mas deve ser utilizado apenas quando não tiver outra opção, em caso de perda de comunicação total durante a auditoria através da ferramenta TIC – Tecnologia da Informação e Comunicação ou similar no notebook. Também é permitido solicitar, à organização auditada, filmagens via aparelho celular ou drones e gravações para permitir que o auditor verifique processos, setores e instalações da organização auditada, bem como realize entrevistas com o pessoal auditado.

8.1.8 - A SAS realiza, antes da auditoria, treinamento/teste para a equipe auditora e para a organização a ser auditada para acessar a ferramenta TIC – Tecnologia da Informação e Comunicação. Conhecimento e habilidade dos membros da equipe auditora em acessar e utilizar a ferramenta de TIC são avaliados neste momento e, caso não seja evidenciada, a SAS procederá a troca da equipe auditora.

8.1.9 - A SAS e a Organização auditada possuem responsabilidades sobre o uso da TIC - Tecnologia da Informação e Comunicação, podendo a auditoria ser interrompida em casos de falha na conexão ou outros fatores que venham a prejudicar o cumprimento dos objetivos da auditoria.

NOTA:
Em caso de auditorias remotas, para a preparação da conclusão, o auditor deve levar em consideração as respostas para as questões apresentadas na reunião de abertura.

8.2 - Comunicação do plano de auditoria

8.2.1 - A comunicação do plano de auditoria com a informação das datas da auditoria, da forma de realização, se remota e/ou presencial, dos processos a serem auditados, dentre outros necessários, previamente acordados com a organização cliente, é realizada através do FORM. 11 - Carta de Comunicação de Auditoria, com antecedência razoável (não menos do que sete dias, exceto em casos de agendamento de última hora ou demora no envio da documentação pela empresa).

8.2.2 - A SAS analisa a viabilidade, riscos e oportunidades para a realização de uma auditoria remota utilizando a TIC - Tecnologia da Informação e Comunicação, através do Diretor de Certificação e da Equipe Auditora SAS, confirmado com a organização cliente no planejamento da auditoria e validado na própria auditoria..

8.2.3 - Em caso de uso da TIC - Tecnologia da Informação e Comunicação, durante auditorias remotas, a SAS e a Organização declaram que definiram previamente os recursos a serem utilizados e avaliaram previamente a habilidade e conhecimento dos envolvidos no seu uso.

8.2.4 - O planejamento de uma auditoria remota inclui:

a) a avaliação e documentação da viabilidade e dos riscos com o auditado;
b) determinar as diferentes TICs utilizadas, preferencialmente “Microsoft Teams” e como serão utilizadas;
c) definir a agenda que pode precisar acomodar disposições diferentes de uma auditoria no local (por exemplo, melhor definição de tarefas por diferentes membros da equipe para garantir que os auditores auditem separadamente e fazer melhor uso do tempo, definição mais detalhada dos temas a serem tratados em diferentes momentos que exigirão uma compreensão melhor e prévia dos processos da organização, etc.);
d) permitir que a organização identifique as pessoas a serem auditadas e garanta sua disponibilidade em um horário definido conforme identificação dos itens a serem auditados.

8.2.5 - Previamente à auditoria, um membro da SAS contata a organização a ser auditada e a equipe auditora de forma a visualizar um teste sobre o uso das TIC, para confirmar que há uma conexão estável e se as pessoas sabem como usar a tecnologia.

8.2.6 - As conclusões, após a análise de riscos e oportunidades, fornecem a base para definir quais processos serão auditados sob quais TICs.

8.2.7 - O auditor também deve confirmar com a organização a viabilidade do método de auditoria remota proposto no programa, com base nas TICs exigidas e no seu conhecimento da organização. Isso inclui a verificação de que as pessoas envolvidas saberão usar a ferramenta. O auditor analisa os riscos e oportunidades determinados à luz dessa auditoria específica e seus objetivos e pode propor alterações no uso determinado das TICs.

8.2.8 - O plano de auditoria irá identificar claramente o que, quando e como a auditoria será conduzida. Nele estão descritos como as TIC serão utilizadas e até que ponto serão usadas para os objetivos da auditoria e para otimizar sua eficácia e eficiência.

8.2.9 - A avaliação e documentação da viabilidade e dos riscos da realização da auditoria de forma remota com o auditado devem ser confirmados pelo auditor lider na reunião de abertura.

8.2.10 - A SAS e a Organização, através da concordância em realizar a auditoria, declaram que analisaram a viabilidade, os riscos e as oportunidades e que eventuais divergências foram previamente resolvidas.

8.2.11 - Em caso de uso de Tecnologias de Informação e Comunicação – TIC, durante auditorias remotas, a SAS e a Organização declaram que definiram previamente os recursos a serem utilizados e avaliaram previamente a habilidade e conhecimento dos envolvidos no seu uso.

8.3 - Comunicação relativa aos membros da equipe auditora

A SAS fornece o nome e, quando solicitado, torna disponíveis informações curriculares de cada membro da equipe auditora, com tempo suficiente para o cliente pedir a substituição de qualquer auditor ou especialista técnico em especial e para a SAS fazer a substituição em resposta a qualquer objeção válida, incluindo ameaças à imparcialidade. Este pedido deverá ser feito em, no máximo, 2 (dois) dias após o recebimento do FORM. 11 - Carta de Comunicação de Auditoria e será apreciado pelo Diretor de Certificação que, concordando, fará as substituições necessárias na equipe auditora.

9 - Auditoria de Certificação inicial

9.1 Generalidades

A auditoria inicial de certificação de um sistema de gestão de segurança da informação será realizada em duas fases: fase 1 e fase 2.

NOTAS:
Pré-Auditoria (opcional):
1 - Opcionalmente para a organização solicitante, a SAS poderá realizar uma pré-auditoria para:
a) Esclarecer à organização sobre o processo de certificação da SAS;
b) Verificar sucintamente o grau de implementação do sistema de gestão de segurança da informação e a compreensão do cliente quanto a norma aplicável.

2 - O dimensionamento do número de auditores necessários a realização da pré-auditoria será acordado entre a SAS e a organização solicitante, porém não será inferior a um dia.

3 - Quaisquer constatações que poderiam ser identificadas como não conformidades na auditoria de certificação, deverão ser relatadas a organização solicitante e registradas como "áreas de preocupação" no FORM. 11.1.

4 - Esta pré-auditoria pode ser realizada de forma remota, utilizando a TIC - Tecnologia da Informação e Comunicação.

9.2 - Fase 1

9.2.1 - O planejamento assegura que os objetivos da fase 1 possam ser atingidos e que o cliente seja informado sobre quaisquer atividades “in-loco” durante a fase 1.

NOTA:
A fase 1 não requer um plano de auditoria formal.

9.2.1.1 - A SAS Certificadora exige que o cliente tome todas as providências necessárias para garantir o acesso aos relatórios de auditoria interna e aos relatórios de revisões independentes da segurança da informação.

9.2.2 - Os objetivos da fase 1 são:

a) analisar a informação documentada do sistema de gestão de segurança da informação do cliente;

b) avaliar as condições específicas da planta do cliente e discutir com o pessoal do cliente, a fim de determinar o grau de preparação para a fase 2;

c) analisar a situação e a compreensão do cliente quanto aos requisitos da norma, em especial com relação à identificação de aspectos-chave ou significativos de desempenho, de processos, de objetivos e da operação do sistema de gestão de segurança da informação;

d) obter as informações necessárias em relação ao escopo do sistema de gestão de segurança da informação, incluindo:

- a(s) planta(s) do cliente;
- processos e equipamento utilizado;
- níveis dos controles estabelecidos (particularmente no caso de clientes i-site);
- requisitos estatutários e regulatórios aplicáveis;

e) analisar a alocação de recursos para a fase 2 e acordar com o cliente os detalhes da fase 2;

f) permitir o planejamento da fase 2, obtendo um entendimento suficiente do sistema de gestão de segurança da informação do cliente e do seu funcionamento no local, no contexto da norma de sistema de gestão ou outro documento normativo;

g) avaliar se as auditorias internas e as análises críticas pela direção estão sendo planejadas e realizadas, e se o nível de implementação do sistema de gestão de segurança da informação demonstra que o cliente está pronto para a fase 2.

NOTAS:
1 - Se ao menos parte da Fase 1 for realizada nas instalações do cliente, isto pode auxiliar a alcançar os objetivos citados acima.
2 - É possível a realização de auditoria Fase 1 nas instalações da SAS e/ou de forma remota utilizando a TIC - Tecnologia da Informação e Comunicação, a critério do Diretor de Certificação, quando as instalações do cliente estiverem localizadas a uma distância da sede da SAS que gere custos adicionais significativos ou em casos em que a organização e/ou a SAS é afetada por algum evento fora de seu controle ou evento de força maior, analisada pela SAS a viabilidade, riscos e oportunidades, desde que os objetivos definidos em “9.2.2” sejam atendidos. A equipe auditora deve registrar o resultado da avaliação dos riscos e oportunidades.
3 - Caso a auditoria da Fase 1 não seja realizada *in loco* (presencial ou remota), tal situação ser justificada pela SAS. Neste caso, a SAS assegura que todas as avaliações aplicáveis para a Fase 1 sejam realizadas até o término da Fase 2. O tempo de auditoria da Fase 1 previsto será fracionado em 50% e a metade acrescida ao tempo da Fase 2.

9.2.3 - As conclusões documentadas com relação ao atendimento dos objetivos da fase 1 e à aptidão para seguir à fase 2 são comunicadas ao cliente, incluindo a identificação de quaisquer áreas de preocupação que poderiam ser classificadas como não conformidades durante a fase 2. Os resultados da fase 1 serão registrados com a utilização do FORM. 11.1 – Relatório de Auditoria.

9.2.4 - Na determinação do intervalo entre as fases 1 e 2, a SAS leva em consideração as necessidades do cliente em resolver as áreas de preocupação identificadas durante a fase 1. Também pode ser preciso que a SAS revise seus preparativos para a fase 2.

Se ocorrerem quaisquer mudanças significativas que impactem o sistema de gestão de segurança da informação, a SAS considera a necessidade de repetir parte ou toda a fase1. O cliente é informado que os resultados da fase 1 podem causar o adiamento ou cancelamento da fase 2.

NOTAS:

1 - Convém que o intervalo entre a fase 1 e a fase 2 seja de no mínimo quinze (15) dias, devendo ser levado em consideração as necessidades do cliente em resolver as áreas de preocupação identificadas durante a Visita Inicial - fase 1 e da SAS em revisar seus preparativos para a auditoria fase 2.

2 - É aceitável realizar as auditorias da fase 1 e da fase 2 sequencialmente, desde que:
- os objetivos individuais de cada fase sejam atendidos, podendo ser identificadas áreas de preocupações na fase 1;
- qualquer constatação feita, independentemente da fase, seja encerrada antes da decisão de certificação. As áreas de preocupações identificadas na fase 1 e não resolvidas serão classificadas como não conformidades na fase 2.
- o nível de implementação do sistema de gestão de segurança da informação verificado na fase 1 comprove que o cliente está pronto para a auditoria fase 2.

3 - Não é recomendado que o tempo decorrido entre as auditorias da fase 1 e da fase 2 seja superior a 3 (três) meses.

4 - Durante a fase 1, a equipe de auditoria deve confirmar o nível de integração do Sistema de Gestão. A SAS revê e modifica, se necessário, o período de duração da auditoria que foi baseado em informações fornecidas na fase de análise da solicitação (IAF MD 11).

5 - Ter uma pessoa da SAS Certificadora que não está envolvida na auditoria revisando o relatório e que decide prosseguir e confirma a competência dos membros da equipe de auditoria para o fase 2 oferece um grau de mitigação para os riscos envolvidos. No entanto, outras medidas de mitigação de risco podem estar em vigor para atingir o mesmo objetivo.

6 - A SAS Certificadora informa o cliente sobre os outros tipos de informações e registros que podem ser necessários para um exame detalhado durante a fase 2.

9.3 - Fase 2

9.3.1 - Com base nas conclusões documentadas no relatório de auditoria da fase 1, a SAS Certificadora deve elaborar um plano de auditoria para a realização da fase 2. Além de avaliar a implementação efetiva do SGSI, o objetivo do fase 2 é confirmar que o cliente adere às suas próprias políticas, objetivos e procedimentos.

Para tal, a auditoria deve centrar-se nos seguintes aspetos:

a) **liderança da alta administração e comprometimento com os objetivos de segurança da informação;**

b) **avaliação de riscos relacionados à segurança da informação; a auditoria deve também assegurar que as avaliações produzem resultados coerentes, válidos e comparáveis, se repetidas;**

c) **determinação de controles com base nos processos de avaliação de riscos de segurança da informação e tratamento de riscos;**

d) **desempenho da segurança da informação e a eficácia do SGSI, avaliando-os em relação aos objetivos de segurança da informação;**

e) **correspondência entre os controles determinados, a Declaração de Aplicabilidade, os resultados da avaliação de risco de segurança da informação, o processo de tratamento de risco e a política e objetivos de segurança da informação;**

f) **Implementação de controlos (ver Anexo E para exemplos de controles de auditoria) tendo em conta o contexto externo e interno e os riscos conexos, bem como a monitorização, medição e análise dos processos e controlos de segurança da informação pela organização, a fim de determinar se os controlos declarados como sendo implementados são efetivamente aplicados e eficazes no seu conjunto;**

g) **programas, processos, procedimentos, registros, auditorias internas e revisões da eficácia do SGSI para garantir que sejam rastreáveis às decisões da alta administração e à política e objetivos de segurança da informação.**
Os resultados da auditoria fase 2 serão registrados com a utilização do FORM. 11.1 – Relatório de Auditoria e FORM. 11.2- Registro de Não Conformidade e comunicados ao cliente.

9.3.2 - A SAS não incentiva a realização de auditoria de certificação (Fase 2) quando a organização cliente e/ou a SAS é afetada por algum evento fora de seu controle ou de força maior que não permita a realização in loco da auditoria completa.

9.3.3 - Escopo da certificação SGSI

9.3.4 - A equipe de auditoria deve auditar o SGSI do cliente coberto pelo escopo definido em relação a todos os requisitos de certificação aplicáveis. A SAS Certificadora confirma, no âmbito do SGSI do cliente, que o cliente atende aos requisitos estabelecidos na ISO/IEC 27001:2022, 4.3.

9.3.5 - A SAS Certificadora garante que a avaliação e o tratamento de riscos de segurança da informação do cliente reflitam adequadamente suas atividades e se estendam aos limites de suas atividades, conforme definido no escopo da certificação. A SAS Certificadora deve confirmar que isso se reflete no escopo do SGSI do cliente. A SAS Certificadora deve verificar se existe uma declaração de confiabilidade para o âmbito da certificação.

9.3.6 - A SAS Certificadora garante que as interfaces com serviços ou atividades que não estejam completamente dentro do escopo do SGSI sejam abordadas no SGSI sujeito a certificação e sejam incluídas na avaliação de risco de segurança da informação do cliente. Um exemplo de tal situação é o compartilhamento de instalações (por exemplo, sistemas de TI, bancos de dados e sistemas de telecomunicações ou a terceirização de uma função de negócios) com outras organizações.

10 - Conclusões da auditoria de certificação inicial

A equipe auditora analisa todas as informações e evidências coletadas durante as fases 1 e 2, a fim de analisar as constatações e concordar quanto às conclusões da auditoria.

11 - Conduzindo auditorias

11.1 - Generalidades

11.1.1 - A SAS tem um processo para realizar auditorias *in loco* (presenciais ou remotas). Esse processo inclui uma reunião de abertura no início da auditoria e uma reunião de encerramento ao final da auditoria e é descrito no documento P0 - Auditores/Técnicos Especialistas - documentos e principais requisitos para realização da auditoria.

11.1.2 - Quando parte da auditoria for realizada de forma remota ou quando o local a ser auditado for virtual, as evidências obtidas durante este tipo de auditoria deverão ser suficientes para permitir que a SAS tome uma decisão consciente sobre a conformidade do requisito em questão. Conhecimento e habilidade dos membros da equipe auditora em acessar e utilizar a ferramenta de TIC – Tecnologia da Informação e Comunicação são avaliados.

NOTA:
É permitido o uso e o registro no relatório de auditoria de informações coletadas por meio de imagens e áudios gerados pela organização auditada em auditorias remotas (através de aparelhos celulares, drones), de forma a permitir que o auditor verifique processos, setores e instalações da organização auditada, bem como realize entrevistas com o pessoal auditado.

11.1.3 - Em uma auditoria remota, é importante que sejam permitidas pequenas interrupções, típicas daquelas que geralmente ocorrem de maneira não planejada em uma auditoria presencial. Também é aceitável que o auditor informe o auditado quando for necessária uma interrupção para ler e analisar as informações fornecidas. Isso permite uma maior compreensão da documentação e evidências apresentadas e a determinação de perguntas adicionais antes da nova reunião.

11.1.4 - A equipe auditora deve solicitar autorização da organização auditada, antes de proceder quaisquer fotos / capturas de tela de documentos ou registros ou outro tipo de evidência.

11.1.5 - Em uma auditoria remota, também é recomendável que informações documentadas que serão analisadas de maneira assíncrona sejam compartilhadas em um sistema seguro e acordado, como nuvem, rede virtual privada ou outros sistemas de compartilhamento de arquivos.

NOTA: Auditorias *in loco* podem incluir acesso remoto a *sites* eletrônicos que contenham informações pertinentes à auditoria do sistema de gestão. Pode ser considerado o uso de meios eletrônicos para a condução de auditorias.

11.2 - Comunicação durante a auditoria

11.2.1 Durante a auditoria, a equipe auditora avalia periodicamente o progresso da auditoria e troca informações. O auditor líder redistribui o trabalho entre os membros da equipe auditora, conforme necessário, e comunica periodicamente o progresso da auditoria e quaisquer preocupações ao cliente.

11.2.2 Quando a evidência disponível da auditoria indicar que os objetivos da auditoria são inatingíveis ou sugerir a presença de um risco imediato e significativo (por exemplo, segurança), o auditor líder relata esse fato ao cliente e, se possível, à SAS, para determinar a ação apropriada. Tal ação pode incluir a reconfirmação ou a modificação do plano de auditoria, mudanças nos objetivos ou no escopo da auditoria ou o encerramento da auditoria. O auditor líder relata o resultado da ação para a SAS.

11.2.3 O auditor líder analisa com o cliente qualquer necessidade de mudanças no escopo da auditoria, que fique aparente com o progresso das atividades da auditoria no local, e relata essas mudanças ao organismo de certificação.

11.2.4 - Em auditorias remotas, o planejamento das atividades leva em consideração a necessidade de acomodar disposições diferentes de uma auditoria no local (por exemplo, melhor definição de tarefas por diferentes membros da equipe para garantir que os auditores auditem separadamente e fazer melhor uso do tempo, definição mais detalhada dos temas a serem tratados em diferentes momentos que exigirão uma compreensão melhor e prévia dos processos da organização, etc.).

11.2.5 - A equipe de auditoria da SAS Certificadora:

a) **exige que o cliente demonstre que a avaliação dos riscos relacionados à segurança da informação é relevante e adequada para a operação do SGSI dentro do escopo do SGSI;**

b) **estabelece se os procedimentos do cliente para a identificação, exame e avaliação de riscos relacionados à segurança da informação e os resultados de sua implementação são consistentes com a política, objetivos e metas do cliente.**

A SAS Certificadora também verifica se os procedimentos utilizados na avaliação dos riscos são sólidos e corretamente aplicados.

11.3 - Identificação e registro das constatações de auditoria

11.3.1 As constatações da auditoria resumindo a conformidade e detalhando as não conformidades, são identificadas, classificadas, registradas e relatadas (ver FORM. 11.1 – Relatório de auditoria e FORM. 11.2 – Registro de não conformidade) para possibilitar uma tomada de decisão de certificação fundamentada ou a manutenção da certificação, baseados em:

a) **um relato da auditoria da análise de risco de segurança da informação do cliente;**

b) **quaisquer conjuntos de controle de segurança da informação usados pela organização para fins de comparação, conforme exigido pela ISO/IEC 27001:2022, 6.1.3 c).**

11.3.2 Oportunidades de melhoria podem ser identificadas e registradas, exceto se proibidas pelos requisitos de um esquema de certificação de sistema de gestão de segurança da informação. Entretanto, as constatações de auditoria que forem não conformidades não são registradas como oportunidades de melhoria.

11.3.3 Uma constatação de não conformidade é registrada contra um requisito específico, e contém uma declaração clara da não conformidade, identificando em detalhes as evidências nas quais a não conformidade se baseia. As não conformidades são discutidas com o cliente para assegurar que a evidência é precisa e que as não conformidades foram compreendidas. Entretanto, o auditor abstém-se de sugerir a causa das não conformidades ou sua solução.

NOTA:
O termo “compreendidas” não significa necessariamente que as não conformidades foram aceitas pelo cliente.

11.3.4 O auditor líder empenha-se em solucionar quaisquer opiniões divergentes entre a equipe auditora e o cliente, relativas às evidências ou constatações da auditoria, e os pontos não resolvidos devem ser registrados.

NOTAS:

Os resultados das auditorias são registrados tendo como base as constatações e evidências da auditoria, obedecendo ao seguinte vocabulário:

1 – Não Conformidade é o não atendimento ao Referencial Normativo, caracterizado pela ausência de um ou mais requisitos do sistema de gestão de segurança da informação ou falha em implementá-los e mantê-los, ou uma situação que vá, com base em evidências objetivas, levantar dúvida quanto à capacidade do sistema de gestão de segurança da informação em atender aos objetivos estabelecidos ou quanto à qualidade dos produtos ou serviços que a organização oferece, impedindo a decisão ou manutenção da certificação.

Não deverá ser registrada não conformidade na fase 1 e, sim, apenas “áreas de preocupação”, se necessário.

1.1 - **Não conformidade maior**: serão classificadas como não conformidades maiores:

- aquela que comprove que o produto/serviço oferecido não atende aos requisitos do cliente e aos requisitos normativos pertinentes;
- falhas sistêmicas no sistema de gestão de segurança da informação (não cumprimento de um requisito inteiro da norma auditada);
- o acúmulo de não conformidades menores em um mesmo item normativo ou;
- a reincidência de uma mesma não conformidade menor identificada em uma auditoria anterior (implementação de ações planejadas para eliminar a não conformidade menor não foi eficaz);
- não realização de auditoria interna ou análise crítica pela direção.

A SAS poderá realizar Auditoria Adicional Complementar para avaliação *in loco* da implementação e eficácia das correções e ações corretivas das não conformidades antes de submeter o processo à decisão de certificação ou Auditoria Adicional Extraordinária para acompanhamento das não conformidades, necessidade de maior amostragem e outros, após a concessão da certificação.
1.2 - **Não conformidade menor**: falha pontual no atendimento e controle de um requisito.

2 - **Oportunidades de Melhoria**: constatações (não aplicáveis a fase 1) focadas nas áreas/processos para possível melhoria do sistema de gestão de segurança da informação.
3 - **Áreas de preocupação**: (constatação exclusiva para Pré-auditoria e fase 1) constatações da Pré-auditoria e da Visita Inicial - fase 1 que poderiam ser classificadas como não conformidade durante a Auditoria de Certificação – fase 2.

11.3.5 - Caso tenham sido utilizados métodos de auditoria à distância, o relatório deve indicar em que medida foram utilizados na realização da auditoria e a sua eficácia na consecução dos objetivos da auditoria.

11.3.6 - Quando as atividades da organização não forem realizadas em um local físico definido e, portanto, todas as atividades da organização forem conduzidas remotamente, o relatório de auditoria deve declarar que todas as atividades da organização são conduzidas remotamente.

11.3.7 - O relatório deve considerar a adequação da organização interna e dos procedimentos adotados pelo cliente para dar confiança no SGSI.

11.3.8 - O relatório inclui um resumo das observações mais importantes, positivas e negativas, sobre a implementação e eficácia dos requisitos do SGSI e dos controles de segurança da informação.

11.4 - Condução da reunião de encerramento

11.4.1 - É realizada uma reunião de encerramento formal, na qual a presença é registrada, com a direção do cliente e, quando apropriado, com o responsável pelas funções ou processos auditados. O objetivo da reunião de encerramento, que normalmente é presidida pelo auditor líder, é, entre outros, apresentar as conclusões da auditoria, incluindo a recomendação relativa à certificação.
As não conformidades são apresentadas de tal maneira que possam ser compreendidas, e acorda-se o prazo para resposta.

11.4.2 - Em casos em que a organização e/ou a SAS é afetada por algum evento fora de seu controle ou evento de força maior, a critério da SAS, o Auditor Líder pode recomendar ou não o adiamento e/ou extensão da validade do certificado por no máximo 6 (seis) meses, inserindo no relatório de auditoria, as justificativas, bem como registrando o risco no relatório de auditoria.

11.4.3 O risco referenciado acima deve ser classificado como **"risco aceitável"** pelo auditor. Isto significa que, não há comprometimento para a decisão da SAS em adiar e/ou estender a validade do certificado, considerando:

- a análise das evidências apresentadas na auditoria remota;
- o número reduzido de auditores.dia e/ou sites auditados;
- o tipo e a complexidade da organização, tais como atividades/serviços administrativos ou atividades de construção, industriais, saúde, mineração, agronegócio, transporte e outros.

11.4.4 - A retroalimentação ou a validação da análise do risco em relação à realização de uma auditoria remota utilizando TIC – Tecnologia da Informação e Comunicação, incluindo sua eficácia e consecução dos objetivos da auditoria é reforçada pelo Auditor Líder. Este pode ter aceito ou não o uso deTIC. Em casos de não possibilidade de realização e/ou continuidade da auditoria e em casos de resultados insatisfatórios ou não eficazes, as justificativas devem ser inseridas no relatório de auditoria.

11.5 - Relatório de auditoria

11.5.1 - A SAS fornece um relatório escrito para cada auditoria ao cliente dentro de um prazo de 10 (dez) dias úteis. A equipe auditora pode identificar oportunidades de melhoria, mas não pode recomendar soluções específicas. A SAS mantém a propriedade pelo relatório de auditoria.

11.5.2 - O auditor líder assegura a preparação do relatório de auditoria, é responsável por seu conteúdo, sendo analisado criticamente pela SAS. O relatório da auditoria fornece um registro preciso, conciso e claro da auditoria para possibilitar uma tomada de decisão de certificação fundamentada.

11.5.3 - Em auditorias remotas, o auditor líder deve confirmar a adequação do plano da auditoria realizada como forma de atualização de dados para análise do risco da SAS para futura auditoria remota utilizando TIC. Isto inclui a eficácia na consecução dos objetivos da auditoria.

11.5.4 - O auditor líder deve confirmar também qualquer outra modificação necessária para futuras auditorias como, por exemplo: escopo da certificação, não aplicabilidade de itens (verificar justificativa), descrição completa do produto, tempo ou data da auditoria, frequência da supervisão, competência da equipe auditora, entre outros.

11.6 - Recomendação da equipe auditora

A recomendação da equipe auditora deverá ser devidamente informada à organização na reunião de encerramento e deverá ser assinalada no Relatório de Auditoria – FORM. 11.1.

11.7 - Análise das causas das não conformidades

A SAS exige que o cliente analise a causa e descreva as correções e as ações corretivas específicas tomadas, ou que planeja tomar, para eliminar as não conformidades detectadas, dentro de um tempo definido (máximo de 90 dias), através do FORM. 11.2 - Registro de não conformidade.

12 - Eficácia das correções e ações corretivas

12.1 - A SAS analisa as correções, as causas identificadas e as ações corretivas apresentadas pelo cliente para determinar se estas são aceitáveis. Esta análise é realizada primeiramente pelo auditor líder. A SAS verifica a eficácia das correções e ações corretivas tomadas. As evidências obtidas para apoiar a solução das não conformidades são registradas.

O cliente é informado sobre o resultado da análise e verificação e também é informado se uma auditoria adicional complementar completa, parcial, ou evidência documentada (a ser confirmada durante futuras auditorias) serão necessárias para verificar a eficácia das correções e ações corretivas.

NOTAS:
1 - A verificação da eficácia de correções e ações corretivas pode ser realizada com base em uma análise da informação documentada fornecida pelo cliente ou, quando necessário, por meio de verificação no local. Normalmente esta atividade é feita por um membro da equipe auditora.
2 - Caso a Correção e/ou Ação Corretiva proposta pela organização no Registro de Não Conformidade ou as evidências de implementação encaminhadas pela organização não estejam completas, o Auditor Líder deverá informar a SAS e, após autorização do Diretor de Certificação, solicitar os documentos faltantes à organização.

12.2 - O auditor deve sempre aprovar as propostas de correção ou ações corretivas, independentemente da classificação da não conformidade.

12.3 - Caso haja necessidade da auditoria adicional complementar, as ações propostas, caso solicitadas, devem ser encaminhadas para análise pelo Auditor Líder antes da realização da auditoria no local.

12.4 - Todas as ações corretivas propostas devem ter sua eficácia evidenciada "in loco" na auditoria subsequente. Neste caso, o Auditor Líder designado para realizar a próxima auditoria na organização deverá realizar o fechamento do registro anotando no campo apropriado.

NOTAS:

1 - Caso na Visita Inicial – fase 1 sejam encontradas áreas de preocupação em relação à(s) norma(s) aplicáveis e em relação à documentação normativa do sistema de gestão de segurança da informação, a organização deverá solucionar as ações de preocupação, sendo a implementação verificada na Auditoria de Certificação – fase 2.

2 – Caso seja recomendada a realização de uma auditoria adicional complementar, a organização deverá implementar a correção e a ação corretiva, **sendo a eficácia verificada nesta Auditoria Adicional Complementar, sempre que possível.**

3 - Apenas após o completo preenchimento dos registros da auditoria, estes serão encaminhados para análise da SAS.

13 - Decisão de certificação

13.1 - Generalidades

A SAS assegura que pessoas (Diretores conforme responsabilidades definidas em sua documentação) que tomam as decisões para concessão ou recusa da certificação, expansão ou redução de escopo da certificação, suspensão ou restauração da certificação, cancelamento ou renovação da certificação sejam diferentes daquelas que realizaram as auditorias. O(s) indivíduo(s) designado(s) para conduzir a decisão da certificação possui (em) a competência apropriada.

13.2 - Ações antes da tomada de decisão

13.2.1 - A SAS tem o processo descrito a seguir para conduzir uma análise eficaz antes da tomada de decisão para concessão da certificação, expansão ou redução de escopo da certificação, renovação, suspensão ou restauração, ou cancelamento da certificação, assegurando que:

a) as informações fornecidas pela equipe auditora são suficientes em relação aos requisitos e ao escopo para certificação;
b) para qualquer não conformidade maior, tenha analisado, aceito e verificado as correções e ações corretivas;
c) para qualquer não conformidade menor, tenha analisado e aceito o plano do cliente para as correções e ações corretivas.

NOTAS:
1 - Esta análise é realizada e registrada pelo Diretor de Certificação em campo apropriado do FORM. 11.1 - Relatório de Auditoria.
2 - Em caso de transferência da certificação emitida por outro organismo de certificação, são avaliadas ainda as informações previstas no item 13.4 abaixo.

13.2.2 - Após o encerramento da auditoria, a SAS deverá encaminhar à organização, o FORM. 11.1 - Relatório de auditoria e, se houver, o FORM. 11.2 - Registro de não conformidade, elaborados pelo auditor líder e analisados pela Diretoria Técnica, dentro do prazo estabelecido.

13.2.3 - Não tendo sido identificadas não conformidades, a Diretoria Técnica fará uma análise do FORM. 11.1 - Relatório de auditoria e encaminhará ao Diretor de Certificação para decisão sobre a certificação.

13.2.4 - Sendo identificadas não conformidades (MAIOR / MENOR), a organização deverá preencher o FORM. 11.2 - Registro de não conformidade com plano para correções e ações corretivas somente para não conformidade MENOR e preencher o FORM. 11.2 - Registro de não conformidade, encaminhando as evidências de implementação da correção e da ação corretiva à SAS somente para não conformidade MAIOR, dentro do prazo acordado. Uma análise destes documentos é realizada pelo auditor líder e posteriormente pela Diretoria Técnica, que encaminhará ao Diretor de Certificação para decisão sobre a certificação.

13.2.5 - As evidências obtidas para apoiar a solução das não conformidades são registradas. O cliente é informado sobre o resultado da análise e verificação. A organização também é informada se uma auditoria adicional complementar ou extraordinária completa, parcial, ou evidência documentada (a ser confirmada durante futuras auditorias) serão necessárias para verificar a eficácia das correções e ações corretivas.

13.2.6 - A data da decisão da certificação é a data identificada na emissão aposta no certificado de conformidade.

13.3 - Informações para concessão da certificação inicial

13.3.1 As informações fornecidas pela equipe auditora a SAS para a decisão sobre a certificação incluem no mínimo:

a) o relatório da auditoria;
b) comentários sobre as não conformidades e, onde aplicável, a correção e ações corretivas tomadas pelo cliente;
c) confirmação das informações fornecidas a SAS usadas na análise crítica da solicitação;

d) confirmação de que os objetivos da auditoria foram alcançados e;
e) uma recomendação de conceder ou não a certificação, juntamente com quaisquer condições ou justificativas/observações.

13.3.2 - O Diretor de Certificação da SAS realizará análise de todo o processo e poderá adotar uma das seguintes decisões:

a) Conceder/ Manter o Certificado de Conformidade;
b) Conceder o Certificado de Conformidade, condicionando a manutenção do mesmo através da realização de uma Auditoria Adicional (Extraordinária) em um prazo máximo de 6 (seis) meses contados a partir da decisão da certificação ou em caso de Auditoria de Supervisão, em um prazo máximo de 6 (seis) meses contados a partir da data de realização da Auditoria de Supervisão;
c) Requerer a apresentação de documentos ou a realização de Auditoria Adicional (Complementar) em um prazo máximo de 90 (noventa) dias contados a partir da data de realização da Auditoria, para solucionar eventuais dúvidas decorrentes do Relatório de Auditoria;
d) Processo interrompido (Negar o Certificado de Conformidade).

13.3.3 - Se a SAS não conseguir verificar a implementação das correções e ações corretivas de qualquer **não conformidade maior** no período determinado, após o último dia da fase 2, a SAS deverá conduzir outra fase 2 ou Auditoria Adicional Complementar.

13.4 - Informações para transferência de certificação

13.4.1 - Para transferência de certificação de outro organismo de certificação, a SAS adotará o processo a seguir para obtenção de informação suficiente de forma a tomar uma decisão sobre a certificação:

13.4.2 - A SAS solicitará o envio prévio dos relatórios de auditoria anteriores e dos registros de não conformidades (se houver) do ciclo de certificação atual para analisar/avaliar a existência ou não de alguma situação específica que impeça a transferência da organização solicitante.

13.4.3 - Poderá ser recomendada a realização de uma pré-visita de transferência para análise da informação documentada fornecida pela solicitante e obtenção de outras informações necessárias.

13.4.4 - A decisão da certificação caberá ao Diretor de Certificação, que realizará a análise do processo após a análise crítica e recomendação da equipe auditora e levará em consideração os seguintes aspectos e evidências documentadas:

(i) confirmação de que as atividades certificadas do cliente estão cobertas e válidas pelo escopo da acreditação da SAS, caso solicitada a acreditação do certificado;

(ii) confirmação de que o escopo acreditado do organismo de certificação emissor está coberto pelo escopo de acreditação do MLA do IAF;

(iii) os motivos que levaram à transferência;

(iv) que o site ou sites que desejam a transferência da certificação possuem uma certificação acreditada válida;

(v) relatórios de auditoria de certificação inicial ou recertificação mais recente e os relatório das auditorias de supervisão do ciclo atual;

NOTA:
Se esses relatórios de auditoria não estiverem disponíveis ou se a auditoria de supervisão ou recertificação não tiver sido finalizada, como exigido pelo programa de auditoria do organismo de certificação emissor, então a organização será tratada como um novo cliente SAS.

(vi) o status de todas as não conformidades críticas evidenciadas nos relatórios ou outros meios disponíveis;

(vii) documentação relevante relacionada ao processo de certificação.

(viii) reclamações recebidas pelo solicitante desde a última auditoria e ações tomadas;

(ix) considerações relevantes para estabelecer um plano de auditoria e um programa de auditoria.

NOTA:
O programa de auditoria estabelecido será revisado pela SAS, se disponibilizado.

(x) qualquer envolvimento atual do cliente a ser transferido com órgãos regulamentadores relevantes para o escopo da certificação em relação à conformidade legal;

(xi) se não há penalidade aplicada por outro organismo de acreditação à organização que requer a transferência, tornando inelegível a certificação ou transferência de organismo de certificação.

13.4.5 - A SAS não aceitará a transferência até que:

(i) tenha sido verificada a implementação de correções e ações corretivas em relação a todas as não conformidades maiores, e
(ii) tenham sido aceitos os planos de correção e ação corretiva para todas as não conformidades menores pendentes do cliente solicitante da transferência.

NOTAS:

1 - Somente certificações cobertas pela acreditação de um signatário do MLA do IAF ou signatário do MLA nível 3 e, onde aplicável, níveis 4 e 5, devem ser elegíveis para transferência. As organizações portadoras de certificações que não estejam cobertas por tais acreditações devem ser tratadas como novos clientes.

2 - Somente certificações acreditadas válidas devem ser transferidas. Certificações que estejam em vias de serem suspensas não devem ser aceitas para transferência.

3 - Em casos onde a certificação foi concedida por um organismo de certificação que tenha cessado a operação ou que a acreditação expirou, esteja suspenso ou cancelado, a transferência deverá ser finalizada no prazo de 90 (noventa) dias a partir da data da decisão do cancelamento do Organismo de Certificação ou no vencimento da certificação, o que vier primeiro. Findo este prazo, os certificados serão considerados cancelados ainda que estejam na validade.

13.5 - Informações para concessão da recertificação

A SAS toma decisões sobre a renovação da certificação com base nos resultados da auditoria de recertificação, bem como nos resultados da análise do sistema, durante o período de certificação, e nas reclamações recebidas de usuários da certificação.

13.6 - Emissão do Certificado

13.6.1 - Se decidido favoravelmente à concessão do Certificado de Conformidade, será emitido o Certificado de Conformidade aplicável e encaminhado à organização. Caso a organização requeira outras cópias, deverá pagar as despesas com a emissão de cópias adicionais.

13.6.2 - O Certificado será controlado através do FORM. 16 - Lista de Organizações Certificadas SAS, propriedade exclusiva da SAS, que também estará acessível ao público através do website da SAS.

14 - Manutenção da Certificação

A SAS mantém a certificação com base na demonstração de que o cliente continua a satisfazer os requisitos da norma de sistema de gestão de segurança da informação. A SAS pode manter a certificação de um cliente baseando-se em uma conclusão positiva pelo líder da equipe auditora sem posterior análise independente e decisão, desde que:

a) para qualquer não conformidade maior ou outra situação que possa conduzir à suspensão ou cancelamento da certificação, a SAS exija que o líder da equipe auditora relate a necessidade de iniciar uma análise crítica por pessoal competente, diferentemente daqueles que realizaram a auditoria, para determinar se a certificação pode ser mantida;

b) pessoal competente da SAS monitore suas atividades de supervisão, incluindo o monitoramento do relatório por seus auditores, para confirmar se a atividade de certificação está operando com eficácia.

NOTA 1: A decisão pela manutenção, expansão ou redução do escopo, renovação, suspensão ou restauração após suspensão, ou cancelamento da certificação é tomada, geralmente, pelo Diretor de Certificação conforme responsabilidades definidas pela SAS.
NOTA 2: A decisão pela manutenção, expansão ou redução do escopo, renovação é registrada no FORM. 11.1 – Relatório de Auditoria e no caso específico da suspensão ou revogação da suspensão, ou cancelamento da certificação é registrada através de carta/e-mail enviado à organização, datada e registrada justificativa.

14.1 - Atividades de supervisão

14.1.1 - Generalidades

14.1.1.1 - A SAS desenvolve suas atividades de supervisão da certificação, a fim de que áreas e funções representativas cobertas pelo escopo dos Sistemas de Gestão de Segurança da Informação sejam monitoradas regularmente e levem em consideração as mudanças em seus clientes certificados e em seus sistemas de gestão.

14.1.1.2 - As atividades de supervisão incluem Auditorias de Supervisão no local para avaliar se o sistema de gestão de segurança da informação do cliente certificado atende aos requisitos especificados em relação à norma na qual a certificação foi concedida. Outras atividades de supervisão podem incluir:

a) consultas da SAS ao cliente certificado sobre aspectos de certificação;

b) análise de quaisquer declarações do cliente com relação às suas operações (por exemplo, material promocional, site na Web);

c) pedidos ao cliente para fornecimento de informação documentada (em papel ou meio eletrônico);

d) análise de informações publicadas na imprensa ou em outras fontes relativas às operações do cliente;

e) análise de reclamações apresentadas quanto às operações do cliente;

f) outros meios de monitorar o desempenho do cliente certificado.

14.2 - Auditoria de supervisão

14.2.1 - Auditorias de supervisão (manutenção) são auditorias no local, mas não são necessariamente auditorias completas do sistema de gestão de segurança da informação e são planejadas junto com outras atividades de supervisão, a fim de que a SAS possa manter a confiança de que o sistema de gestão certificado continua a atender aos requisitos entre as Auditorias de Recertificação. A supervisão para a norma de sistema de gestão de segurança da informação inclui:

a) auditorias internas e análise crítica pela direção;

b) uma análise das ações tomadas para as não conformidades identificadas durante a auditoria anterior,

c) gestão de reclamações,

d) eficácia do sistema de gestão de segurança da informação com respeito ao alcance dos objetivos do cliente certificado e os resultados pretendidos do(s) respectivo(s) sistema(s) de gestão;

e) progresso de atividades planejadas visando a melhoria contínua,

f) controle operacional contínuo,

g) análise de quaisquer mudanças, e

h) uso de marcas e/ou quaisquer outras referências à certificação.

NOTA:
Nas auditorias de sistema de gestão integrados, a SAS confirma se o nível de integração mantém-se inalterado durante todo o ciclo de certificação para assegurar que as durações de auditoria estabelecidas ainda são aplicáveis (IAF MD 11).

14.2.2 – A primeira Auditoria de Supervisão do cliente após a concessão de certificação do primeiro ciclo de certificação de 3 (três) anos deve ser realizada no máximo 1 (hum) ano após a data da concessão de certificação. As demais Auditorias de Supervisão convém ser realizadas no máximo anualmente, até na data da concessão da certificação ou recertificação anterior, podendo ser postergadas se devidamente justificadas, porém sendo obrigatório a realização de ao menos uma auditoria dentro de cada ano calendário de vigência do certificado.

14.2.3 – Para auditorias de sistema de gestão de segurança da informação NBR ISO/IEC 27001, a SAS deve receber o Questionário de Avaliação Preliminar – FORM. 7 para análise e realização do agendamento da auditoria de supervisão, bem como qualquer alteração do Contrato Social ou Estatuto da organização que tenha ocorrido desde a última auditoria.

14.2.4 – Em caso de alteração do Contrato Social ou Estatuto, essa documentação poderá ser solicitada à organização pelo auditor líder para análise, quando da realização da auditoria de supervisão, conforme FORM. 8 – Lista de documentos da empresa solicitante.

14.2.5 – Caso, 30 (trinta) dias antes do prazo previsto a organização não agende a data da auditoria, a SAS informa a data máxima de realização, tendo em vista as sanções previstas neste Regulamento. Independente do contato da SAS com a organização, a responsabilidade pela realização da Auditoria de Supervisão dentro do prazo previsto é da organização certificada.

14.2.6 – Em não se submetendo à auditoria de supervisão na data máxima de realização informada, a empresa será suspensa pelo prazo de 180 (cento e oitenta) dias. Neste período, ela poderá realizar a auditoria de supervisão de forma a não ocasionar o cancelamento da certificação.

14.2.7 - **Auditorias de supervisão durante evento fora do controle da SAS ou de força maior.**

14.2.7.1 - **Para a primeira auditoria de supervisão após a certificação de sistemas de gestão**, a SAS avalia o risco de não realizar esta auditoria no prazo previsto no programa e toma a decisão apropriada.

14.2.7.2 - **Para outras auditorias de supervisão de sistemas de gestão,** caso os eventos de força maior ou fora do controle da SAS impeçam a realização desta auditoria dentro do ano calendário previsto, a SAS avalia o risco e toma a decisão apropriada.

14.2.7.3 - Uma análise cuidadosa da viabilidade da realização da auditoria presencial, do adiamento ou da realização de auditoria remota (total ou parcial) para avaliar a conformidade da organização é realizada pela SAS.

14.2.7.4 - Após primeira análise, para a avaliação da viabilidade e dos riscos da realização de forma remota ou adiamento de uma auditoria quando a organização certificada e/ou a SAS é afetada por algum evento fora de seu controle ou de força maior, a SAS obtém da organização certificada, como parte da avaliação de riscos, respostas para as questões sobre a situação da operação da organização. Esta informação é solicitada por e-mail antes da emissão da Carta de Comunicação de Auditoria (Plano de Auditoria).

NOTA:
A SAS informa à equipe auditora, as respostas às questões sobre a situação da operação da organização para que sejam confirmadas na reunião de abertura da auditoria, quando for realizada auditoria.

14.2.7.5 – Nos casos citados anteriormente, a SAS solicita previamente à organização certificada o envio das informações documentadas abaixo.

- do relatório da auditoria de certificação - Fase 2 ou de supervisão anterior (como aplicável);
- do relatório da última auditoria interna;
- da ata de análise crítica da direção da organização;
- de evidências de implementação das correções e ações corretivas de eventuais não conformidades menores;
- da retroalimentação e reclamação de clientes.

14.2.7.6 - Caso a SAS conclua que o risco do adiamento previsto no quadro anterior é **ACEITÁVEL** e que a situação que gerou o adiamento possa ser solucionada até seis meses após o prazo normal de realização desta auditoria, concede um prazo extra para que a auditoria de supervisão seja realizada.

14.3 - Recertificação

14.3.1 - Planejamento da auditoria de recertificação

14.3.1.1 - O propósito da auditoria de recertificação é confirmar a conformidade e a eficácia contínuas do sistema de gestão de segurança da informação como um todo, e a sua contínua relevância e aplicabilidade ao escopo de certificação.

Uma auditoria de recertificação é planejada e realizada para avaliar a continuação do atendimento a todos os requisitos da norma pertinente de sistema de gestão ou outro documento normativo.

A mesma é planejada e conduzida em tempo hábil para permitir uma renovação oportuna antes da data de expiração do certificado.

14.3.1.2 - A atividade de recertificação inclui a análise dos relatórios de auditoria de supervisão anteriores e considera o desempenho do sistema de gestão de segurança da informação durante o ciclo de certificação mais recente.

14.3.1.3 - Nas atividades de auditoria de recertificação, pode ser necessário realizar uma fase 1 em situações onde houver mudanças significativas no sistema de gestão de segurança da informação, na organização ou no contexto no qual o sistema de gestão de segurança da informação opera (por exemplo, mudanças na legislação).

14.3.2 - Auditoria de recertificação

14.3.2.1 - A auditoria de recertificação inclui uma auditoria no local que considere os seguintes tópicos:

a) a eficácia de todo o sistema de gestão de segurança da informação, considerando mudanças internas e externas, e sua relevância e aplicabilidade contínuas ao escopo de certificação;

b) comprometimento demonstrado para manter a eficácia e melhoria do sistema de gestão de segurança da informação, a fim de melhorar o desempenho global;

c) a eficácia do sistema de gestão de segurança da informação em relação a atingir os objetivos do cliente certificado e os resultados esperados do(s) respectivo(s) sistema(s) de gestão.

14.3.2.2 - Convém que a auditoria de recertificação seja realizada ao menos 60 (sessenta) dias antes da expiração da certificação de forma a haver tempo hábil para permitir a análise do relatório de auditoria, o tratamento de eventuais não conformidades, a tomada de decisão e a emissão do certificado antes expiração da certificação do cliente.

14.3.2.3 - Para qualquer não conformidade MAIOR, a SAS define limites de tempo para correção e ações corretivas. Estas ações devem ser implementadas e verificadas antes da expiração da certificação.

14.3.2.4 - Quando as atividades de recertificação são completadas com sucesso antes da data de expiração da certificação vigente, a data de expiração da nova certificação pode ser baseada na data de expiração da certificação vigente. A data de emissão no novo certificado deve ser a partir da decisão de recertificação.

14.3.2.5 - Após a expiração da certificação, a SAS pode restaurar a certificação em até seis meses, desde que as atividades pendentes sejam completadas em até seis meses, senão no mínimo uma fase 2 deve ser conduzida em até 12 meses após a expiração da certificação.

A data efetiva no certificado deve ser a partir da decisão da recertificação e a data de expiração deve se basear no ciclo de certificação anterior.

NOTA:
A SAS toma decisões sobre a renovação da certificação com base nos resultados da Auditoria de Recertificação, bem como nos resultados da análise do sistema, durante o período de certificação, e nas reclamações recebidas de usuários da certificação.

14.3.3 Auditoria de recertificação durante evento fora do controle da SAS ou de força maior

14.3.3.1 - Caso a auditoria de recertificação não possa ser realizada em prazo que permita o encerramento do processo de recertificação antes do vencimento do certificado, em função de algum evento fora de seu controle ou de força maior, a SAS avalia o risco de emitir um novo certificado para a organização, estendendo o prazo de validade da certificação em até seis meses, dentro dos quais deve ser realizada a auditoria de recertificação completa, da seguinte forma:

1. Preferencialmente através da realização de uma auditoria adicional extraordinária, realizada de forma remota, por um auditor líder qualificado para a norma de referência, na qual devem ser avaliados no mínimo os seguintes requisitos:
    - Auditoria Interna
    - Indicadores dos objetivos
    - Análise Crítica pela direção
    - Não conformidades e ações implementadas no período
    - Ações para abordar riscos e oportunidades (incluindo o evento que causou o adiamento da auditoria)
    - Evidências de implementação de ações decorrentes de não conformidades da auditoria anterior (caso aplicável)
    - Reclamação de clientes

2. Caso não seja possível realizar a auditoria remota descrita no item 1, a SAS avalia o risco através da análise:
    - do relatório da última auditoria de supervisão realizada;
    - do relatório da última auditoria interna e
    - do registro da análise crítica da direção da organização.

- de evidências de implementação das correções e ações corretivas de eventuais não conformidades menores;
- da retroalimentação e reclamação de clientes.

14.3.3.2 - Caso a SAS conclua, através de uma das formas acima,

- que o risco de estender a certificação da organização, sem a realização de uma auditoria de recertificação completa, por até seis meses é **aceitável** e
- que a situação que gerou o adiamento possa ser solucionada até seis meses após o vencimento do certificado vigente,
- a SAS concede a recertificação por este prazo e emite um novo certificado.

14.3.3.3 - Na situação acima, a emissão do certificado para todo o ciclo de 3 anos é condicionada ao encerramento do processo de recertificação dentro deste prazo de seis meses, mantendo-se o ciclo (de 3 anos) a partir da validade do certificado anterior.

14.4 - Auditorias especiais

14.4.1 - Expansão de escopo

14.4.1.1 - A SAS, em resposta a uma solicitação para expansão de escopo de uma certificação já concedida, realiza uma análise crítica da solicitação, por meio de seu Diretor de Certificação, e determina quaisquer atividades de auditoria são necessárias para decidir se a extensão pode ou não ser concedida. Esta Auditoria Especial, também pode ser chamada de Auditoria Adicional Complementar e poderá ser realizada em conjunto com as Auditorias de Supervisão ou Auditorias de Recertificação.
14.4.1.2 – Tanto para a solicitação de extensão quanto para a redução de escopo, a SAS deverá:

a) Fazer alteração no Certificado de Conformidade os quais terão as seguintes características:

- Numeração: será repetido o mesmo número do original acrescido do seqüencial alfabético (A, B, C... etc);
- Data: será colocada a data da nova decisão/emissão;
- Validade: permanecerá a validade do Certificado;

b) Colocar no verso do novo Certificado uma observação contendo a(s) razão(ões) que motivou(aram) a alteração ou emenda ao certificado;

c) Solicitar à organização, caso necessário, a devolução do Certificado que está sendo substituído.

14.4.2 - Auditorias avisadas com pouca antecedência / Atividades de vigilância

Pode ser necessário para a SAS realizar auditorias avisadas com pouca antecedência ou sem aviso em clientes certificados para investigar reclamações ou em resposta a mudanças ou como acompanhamento de mercado. Em tais casos:

a) a SAS descreverá e avisará antecipadamente ao cliente certificado as condições nas quais essas auditorias serão realizadas;

b) a SAS toma um cuidado adicional ao designar a equipe auditora, devido à falta de oportunidade para o cliente recusar algum membro da equipe auditora.

NOTA:
Na escolha da amostragem para acompanhamento de mercado dos clientes certificados, a SAS analisa, dentre outros: o número de não conformidades nas últimas auditorias / análise de relatório de auditoria; reclamações de clientes realizadas diretamente à SAS ou em notícias/sites.

14.4.3 **- Os procedimentos de auditoria de vigilância são um subconjunto daqueles para a auditoria de certificação do SGSI do cliente, conforme descrito nesta Pb.**
O objetivo da vigilância é verificar se o SGSI aprovado continua a ser implementado, considerar as implicações das mudanças no SGSI iniciadas como resultado de mudanças nas práticas operacionais do cliente em confirmar a conformidade contínua com os requisitos de certificação. Os programas de auditoria de vigilância abrangerão
pelo menos:
a) **os elementos de manutenção do SGSI, como avaliação de risco de segurança da informação e manutenção de controle, auditoria interna do SGSI, revisão da gestão e ação corretiva;**
b) **comunicações de partes externas, conforme exigido pela ISO/IEC 27001 e outros documentos exigidos para certificação.**

14.4.4 **No mínimo, todas as auditorias de vigilância efetuadas pela SAS Certificadora analisa o seguinte:**
a) **a eficácia do SGSI no que diz respeito ao alcance dos objetivos da política de segurança da informação do cliente;**
b) **o funcionamento de procedimentos para a avaliação e revisão periódica da conformidade com a legislação e regulamentação relevantes em matéria de segurança da informação;**
c) **alterações aos controlos determinados e alterações resultantes à declaração de fidelidade;**
d) **Execução e eficácia dos controlos indicados no programa de auditoria.**

14.4.4.1 **A SAS Certificadora é capaz de adaptar seu programa de atividades de vigilância para refletir as questões de segurança da informação relacionadas a riscos e impactos sobre o cliente e justificar esse programa.**

As auditorias de vigilância podem ser combinadas com auditorias de outros sistemas de gestão. Os relatórios de auditoria devem indicar claramente os aspetos relevantes para cada sistema de gestão.

Durante as auditorias de vigilância, a SAS Certificadora verifica os registos dos recursos e reclamações apresentados aa SAS Certificadora. Quando qualquer não conformidade ou falha no cumprimento dos requisitos de certificação for revelada, a SAS Certificadora verifica se o cliente investigou seu próprio SGSI e procedimentos e tomou as medidas corretivas apropriadas.

O relatório de vigilância contém, em especial, informações sobre a eliminação das não conformidades reveladas anteriormente, a versão da declaração de fiabilidade e as alterações importantes em relação à auditoria anterior.

14.5 - Procedimento para Suspensão, Cancelamento ou Redução do Escopo de Certificação

14.5.1 - A SAS considera como falta grave aquela cometida por uma organização certificada que tenha realizado uma ou mais das seguintes condutas:

a) adulteração de qualquer informação que conste do Certificado de Conformidade;

b) alteração no seu sistema de gestão de segurança da informação sem comunicação imediata à SAS, tais como: alteração de sua estrutura organizacional, alteração significativa de sua equipe técnica, mudança de sistemática de funcionamento, etc. Estas modificações poderão conduzir a uma reavaliação, que poderá incluir os serviços de Auditoria, cujo custo será absorvido pela organização certificada;

c) divulgação de informação enganosa quanto aos dados do seu Certificado de Conformidade;

d) realização de produto ou prestação de serviço sem observar os preceitos da gestão de segurança da informação e as exigências do seu sistema de gestão de segurança da informação, que causem riscos à segurança e à saúde das pessoas que trabalham na organização, aos circunvizinhos e aos futuros usuários do empreendimento, serviço ou produto;

e) omissão de dados e informações necessárias ao dimensionamento e planejamento das atividades de certificação, tais como: numero de trabalhadores, número de escritórios, número de obras, número de projetos, número de contratos de gerenciamento de empreendimentos, etapas de produção no canteiro de obras, localidades ou instalações envolvidas no escopo de certificação, entre outros.

f) falha persistente ou seriamente do sistema de gestão de segurança da informação certificado em atender aos requisitos de certificação, incluindo os requisitos para a eficácia do sistema de gestão;

g) não permissão, por parte da organização certificada, que as Auditorias de Supervisão, Adicional Complementar, Adicional Extraordinária ou de Recertificação sejam realizadas nas freqüências exigidas.

h) não cumprimento de obrigações financeiras e demais despesas pertinentes e relacionadas com o contrato e seu objeto.

i) não notificação imediata à SAS sobre qualquer incidente ou quebra de regulamentação relativa ao escopo do certificado que exija o envolvimento da autoridade regulatória competente, nos casos em que possa ser demonstrado que o sistema de gestão falhou seriamente em atender aos requisitos da certificação.

14.5.2 - Para toda falta grave cometida por parte de uma organização aos procedimentos da SAS, e ao contrato correspondente, sem prejuízo do disposto neste capítulo, poderá ser aplicada as seguintes sanções:

a) Advertência privada;

b) Suspensão parcial ou integral por prazo máximo de 6 (seis) meses (sem rescisão de contrato);

d) Cancelamento ou Redução do Escopo (com rescisão de contrato ou emissão de novo contrato com redução do escopo).

NOTA:
No caso de certificação em sistemas de gestão integrados, se a certificação de um ou mais sistema norma de gestão/especificação está sujeito à suspensão, redução ou cancelamento, a SAS investiga o impacto deste sobre a certificação para outra norma de sistema de gestão / especificação (IAF MD 11).

14.5.3 - A SAS suspende a certificação nos casos em que, por exemplo:

- o sistema de gestão de segurança da informação da organização certificada falhou persistentemente ou seriamente em atender aos requisitos de certificação, incluindo os requisitos para a eficácia do sistema de gestão;
- o cliente/organização certificada não permitiu que auditorias de supervisão ou de recertificação sejam realizadas nas frequências exigidas;
- o cliente/organização certificada solicitou voluntariamente uma suspensão;
- o cliente não pagou a SAS as taxas constantes na proposta técnica-comercial, bem como todas as demais despesas pertinentes e relacionadas com o contrato e seu objeto;

- o cliente/organização certificada não permitiu o acesso dos avaliadores da Cgcre (Coordenação Geral de Acreditação) em suas instalações e dependências quando da realização das auditorias testemunhas e não permitiu o acesso da Cgcre e SAS em suas instalações e dependências nas ações de acompanhamento de mercado.

14.5.4 - Durante a suspensão, a certificação do sistema de gestão de segurança da informação do cliente fica temporariamente inválida.

14.5.5 - A SAS restaura a certificação suspensa se o problema que resultou na suspensão foi resolvido. A falha na resolução dos problemas que ocasionaram a suspensão, no prazo estabelecido pelo organismo de certificação, resultará no cancelamento ou na redução do escopo da certificação.

NOTA: Na maioria dos casos, a suspensão não ultrapassa 6 (seis) meses.

14.5.6 - A SAS reduz o escopo de certificação do cliente para excluir as partes que não atendam aos requisitos, quando o cliente tiver falhado persistentemente ou seriamente em atender aos requisitos de certificação para aquelas partes do escopo da certificação. Qualquer redução desse tipo deve estar de acordo com os requisitos da norma usada para certificação.

14.5.7 - A concessão do Certificado de Sistemas de Gestão de Segurança da Informação e do direito de uso da Marca SAS de Organização Certificada não substituem, em caso algum, a garantia que corresponde à organização nos termos da Lei.

14.5.8 - O uso abusivo do Certificado e da Marca SAS de Organização Certificada pela organização, poderá acarretar a tomada de ações pela SAS podendo incluir pedidos para correção e ação corretiva, as sanções previstas neste procedimento, publicação da transgressão e, se necessário, ação legal.

14.5.9 - As sanções serão aplicadas por determinação do Diretor de Certificação ou Conselho de Certificação da SAS, que deverá notificar a organização através de carta registrada ou e-mail.

14.5.10 - Será assegurado à organização que receber a sanção, exceto em casos de solicitação voluntária de suspensão, o direito de defesa por escrito, no prazo máximo de 30 (trinta) dias a partir do recebimento da notificação, observando que a defesa não terá efeito suspensivo.

14.5.11 - A SAS poderá realizar Auditoria Adicional Complementar nos casos de suspensão juntamente com a Auditoria de Supervisão ou Recertificação, caso aplicável, para verificar a eficácia da implementação da correção e da ação corretiva para a(s) não conformidade(s) dentro do prazo máximo estabelecido para a suspensão.

14.5.12 - Caso após algum evento fora de controle ou evento de força maior, a SAS não consiga contato com uma organização certificada, deve proceder normalmente quanto à suspensão e cancelamento dos certificados.

14.5.13 - No caso de cancelamento ou redução do escopo (independente de como foi determinado), a organização deverá se abster de continuar promovendo a certificação e, caso necessário, devolver todos os documentos de certificação exigidos pela SAS.

14.5.14 - A revogação das sanções, caso aplicável, serão aplicadas por determinação do Diretor de Certificação ou Conselho de Certificação da SAS, que deverá notificar a organização através de carta registrada ou e-mail.

14.5.15 - A SAS possui Contrato de Certificação com validade jurídica com o cliente certificado em relação às condições de cancelamento, assegurando que, quando avisado do cancelamento da certificação, o cliente interrompa o uso de todo material publicitário que faça referência à situação de organização certificada.

15 - Processo de Tratamento de Apelações

15.1 - A SAS possui o processo documentado abaixo para receber, avaliar e tomar decisões sobre apelações.

NOTA:
A SAS torna acessível ao público o procedimento para tratamento de apelações nos Regulamentos Gerais da Certificação – Pb e no site www.sascertificadora.com.br.

15.2 - A SAS, é responsável por todas as decisões em todos os níveis do processo de tratamento de apelações e assegura que as pessoas envolvidas neste processo sejam diferentes daquelas que realizaram as auditorias e tomaram as decisões de certificação (ver item 13.1).

15.3 - A submissão, investigação e decisão sobre apelações não poderão resultar em nenhuma ação discriminatória contra o apelante.

15.4 - As apelações poderão ser apresentadas a SAS pelas organizações clientes, por escrito e devidamente fundamentadas no prazo máximo de 10(dez) dias a partir do recebimento do relatório de auditoria.

15.4.1 - Após a validação das apelações apresentadas pelo Diretor de Certificação ou pela Diretora Técnica, inicia-se o processo de investigação, consultando a outra parte envolvida.

15.4.2 - É assegurado o direito de defesa para as apelações, através de notificação à outra parte que também deverá ser apresentada por escrito no prazo máximo de 10 (dez) dias a partir do recebimento de notificação.

15.4.3 - Para a tomada de decisão, a SAS considera os resultados de apelações anteriores similares.

15.4.4 - A SAS mantém os registros das apelações através do FORM. 17 – Registro de Apelação e Reclamação, possibilitando o rastreamento das apelações, incluindo as ações tomadas para solucioná-las.

15.4.5 - Caso validada, a SAS garante a implementação de correções e ações corretivas apropriadas, podendo ser:

- o cancelamento total ou parcial da não conformidade;
- a revisão da redação da não conformidade;
- a orientação ao pessoal envolvido nas atividades de certificação pertinentes.

15.5 - A SAS, que recebe a apelação, será responsável por coletar e verificar toda a informação necessária para validar a apelação.

15.6 - A SAS confirma o recebimento da apelação e fornece ao apelante, informações de andamento e o resultado da apelação.

15.7 - A decisão a ser comunicada ao apelante é tomada, ou revisada e aprovada, por pessoa sem envolvimento anterior com o assunto da apelação.

15.7.1 - As apelações serão resolvidas pelo Diretor de Certificação ou pela Diretora Técnica, respeitado o disposto neste documento.

15.7.2 - As apelações pertinentes às atividades e/ou decisões do Diretor de Certificação serão resolvidas pela Diretora Técnica e/ou pelo Conselho de Certificação, conforme natureza da apelação.

15.7.3 - As apelações pertinentes às atividades e/ou decisões da Diretora Técnica serão resolvidas pelo Diretor de Certificação, e/ou pelo Conselho de Certificação, conforme natureza da apelação.

15.8 - O apelante será comunicado formalmente da decisão final e término do processo relativo às apelações, decisão esta, tomada, ou revisada e aprovada, por pessoa(s) sem envolvimento anterior com o assunto das apelações.

16 - Processo de Tratamento de Reclamações

16.1 - A SAS é responsável por todas as decisões em todos os níveis do processo de gestão de reclamações.

16.2 - A SAS assegura que a submissão, investigação e decisão sobre reclamações não resultem em quaisquer ações discriminatórias contra o reclamante.

16.3 - Ao receber as reclamações, a SAS deverá confirmar se as mesmas estão relacionadas com atividades de certificação pelas quais é responsável e, se estiverem, deve tratá-las. Se as reclamações forem relativas a um cliente certificado, o exame das reclamações deverá incluir a análise da eficácia do sistema de Gestão Empresarial de Serviços Notariais e de Registros certificado.

16.4 - Quaisquer reclamações sobre um cliente certificado deverão ser comunicadas pela SAS ao cliente certificado em questão em um tempo adequado.

16.5 - A SAS descreve, neste capítulo, o processo para receber, avaliar e tomar decisões sobre reclamações. Este processo está sujeito aos requisitos de confidencialidade em relação ao reclamante e ao assunto da reclamação.

16.5.1 - As reclamações poderão ser apresentadas à SAS pelas organizações certificadas ou outras partes, por escrito e devidamente fundamentadas.

NOTA:
A SAS torna acessível ao público o procedimento para tratamento de reclamações nos Regulamentos Gerais da Certificação – Pb e no site www.sascertificadora.com.br.

16.6 - O processo de tratamento de reclamações da SAS inclui pelo menos os seguintes elementos e métodos:

a) uma descrição geral do processo de recebimento, validação e investigação da reclamação, e da decisão de quais ações serão tomadas em resposta a ela;

b) rastreamento e registro de reclamações, incluindo as ações tomadas em resposta a elas;

c) garantia de que quaisquer correções e ações corretivas apropriadas sejam tomadas.

16.7 - A SAS, ao receber a reclamação, é responsável pela coleta e verificação de todas as informações necessárias para validar a reclamação.

16.8 - Sempre que possível, a SAS confirma o recebimento das reclamações e fornece ao reclamante informações sobre o andamento e o resultado do processo.

16.8.1 - É assegurado o direito de defesa para as reclamações, através de notificação à outra parte que também deverá ser apresentada por escrito no prazo máximo de 10 (dez) dias a partir do recebimento de notificação.

16.9 - A decisão a ser comunicada ao reclamante é preparada, ou revisada e aprovada, por pessoa(s) sem envolvimento anterior com o assunto das reclamações.

16.9.1 - As reclamações serão resolvidas pelo Diretor de Certificação ou pela Diretora Técnica.

16.9.2 - As reclamações pertinentes às atividades e/ou decisões do Diretor de Certificação serão resolvidas pela Diretora Técnica e/ou pelo Conselho de Certificação, conforme natureza da reclamação.

16.9.3 - As reclamações pertinentes às atividades e/ou decisões da Diretora Técnica serão resolvidas pelo Diretor de Certificação e/ou pelo Conselho de Certificação, conforme natureza da reclamação.

16.9.4 - Caso aplicável, a SAS poderá aplicar as sanções descritas no item 14.5.2.

16.10 - Sempre que possível, a SAS enviará ao reclamante uma notificação formal do término do processo de tratamento da reclamação.

NOTA:
A SAS mantém os registros das reclamações através do FORM. 17 - Registro de apelação e reclamação, que inclui ações tomadas para solucioná-las, quaisquer correções, ações corretivas ou preventivas tomadas e avalia sua eficácia.

16.11 - A SAS determina, junto com o cliente certificado e o reclamante, se ele deve tornar públicos o assunto da reclamação e a sua solução e, se assim for, em que extensão.

16.12 - Caso a análise de uma reclamação ou outra qualquer informação indicar que a organização certificada não mais atende aos requisitos da certificação, a SAS também poderá, à critério do Diretor de Certificação ou Diretora Técnica, realizar Auditoria Adicional Complementar para verificar a implementação das correções e ações corretivas ou poderá aplicar as sanções previstas neste Regulamento.

17 - Imparcialidade

17.1 - A SAS realiza suas atividades baseada em princípios para inspirar confiança, não permitindo a existência de situações que configurem ameaça à imparcialidade, ou seja, deve haver a presença real e perceptível de objetividade, implicando na ausência de conflitos de interesse ou a sua resolução de modo a não influenciar de forma adversa as atividades subseqüentes da SAS.

17.2 - Observando-se o princípio da imparcialidade, configuram conflitos de interesse, situações em que um ou mais membros do Conselho de Certificação, da Equipe Auditora, além de todos os que estiverem ligados à SAS por vínculos empregatícios tenham:

a) parentesco até o segundo grau, com administradores da organização solicitante ou com acionistas que tenham um percentual significativo, no seu controle acionário;

b) participação acionária na organização solicitante;

c) esteja prestando serviços de qualquer tipo à solicitante;

d) participado da implementação e/ou desenvolvimento de Sistemas de Gestão de Segurança da Informação da organização solicitante, nos últimos três (3) anos.

17.3 - Conflitos de interesse

17.3.1 - A SAS Certificadora pode acrescentar valor durante as auditorias de certificação e supervisão (por exemplo, identificando oportunidades de melhoria, à medida que se tornam evidentes durante a auditoria, sem recomendar soluções específicas) sem que tal seja considerado uma consultoria ou que tenha um potencial conflito de interesses.

17.3.2 - A SAS Certificadora não deve fornecer análises internas de segurança da informação do SGSI do cliente sujeito a certificação. Além disso, a SAS Certificadora é independente do organismo ou organismos (incluindo quaisquer indivíduos) que prestam a auditoria interna do SGSI.

18 - Requisitos para referência à Certificação, Uso do Certificado e da Marca SAS de Organização Certificada

18.1 - A SAS possui regras para gerir qualquer marca de certificação de sistema de gestão de segurança da informação que ela autorize os clientes certificados a usar. Estas regras asseguram, entre outros aspectos, a rastreabilidade a SAS.

18.2 - Não deve existir ambigüidade na marca ou no texto que a acompanha, em relação ao que foi certificado e à qual organismo concedeu a certificação.

18.3 - A Marca SAS de Organização Certificada **não deve ser usada** em um produto nem na embalagem (primária ou secundária) do produto nem de qualquer outra maneira que possa ser interpretada como denotando conformidade do produto. Na embalagem poderá haver declaração (ver 18.8 e 18.10).

18.4 - A organização deverá encaminhar à Diretoria de Certificação da SAS, o material a ser divulgado referente à certificação de Sistemas de Gestão de Segurança da Informação SAS, para autorização, antes de sua divulgação para impressão em gráfica, distribuição ou publicação em meios de comunicação tais como internet, folhetos ou propaganda, ou outros documentos.

18.5 - Se a SAS autorizar o direito de uso de uma logomarca para indicar a certificação de um sistema de gestão de segurança da informação, a organização pode usar esta logomarca especificada somente conforme autorizado pela SAS. Esta logomarca **não poderá ser usada** em um produto, ou de modo a poder ser interpretado como denotando conformidade do produto.

18.6 - A SAS **não permite** que sua Marca SAS de Organização Certificada seja aplicada a relatórios de laboratórios referentes a ensaio, calibração ou inspeção ou certificados.

18.7 - A SAS possui regras para gerir o uso de qualquer declaração, na embalagem ou nas informações que acompanham o produto, que o cliente certificado possui um sistema de gestão certificado.

18.8 - A SAS não permite o uso de declaração no produto de que o sistema de gestão é certificado. É permitido o uso de tal declaração na embalagem (ver nota abaixo).

NOTAS:
1 - Embalagem do produto é considerada aquela que pode ser removida sem que o produto seja desintegrado ou danificado.
2 - Informações que acompanham o produto são consideradas como disponíveis separadamente ou facilmente destacadas.
3 - Rótulos ou placas de identificação são consideradas parte do produto.

18.9 - A declaração **não pode inferir** que o produto, processo ou serviço seja certificado.

18.10 - A declaração **deverá** incluir referência aos três itens abaixo:
- identificação (ex. marca ou nome) do cliente certificado;
- o tipo de sistema de gestão (ex., segurança da informação, qualidade, ambiental) e a norma aplicável;
- identificação da SAS.

18.11 - A tabela abaixo provê um resumo referente ao uso da Marca SAS de Organização Certificada ou declaração para indicar quando um produto/serviço foi feito ou realizado sob um sistema de gestão de segurança da informação certificado:

	No produto, incluindo rótulos e placas de identificação (*a).	**Na embalagem (*b) ou nas informações que acompanham o produto.**
Uso da Marca (*c)	Não permitido	Não permitido
Uso da declaração (*d)	Não permitido	Permitido

*a) Pode ser o próprio produto tangível ou um produto em uma embalagem individual, caixa, etc. No caso de atividades de ensaio/análise, pode ser um relatório de ensaio/análise.

*b) É considerado produto e não embalagem se, ao ser removido, o produto se desintegre ou se danifique.

*c) Aplica-se para a marca apresentada em uma forma específica. Uma declaração somente em palavras não constitui uma marca. Tal declaração deve ser verdadeira e não induzir a erro.

*d) A declaração pode ser uma afirmação declarando que "(Este produto) foi fabricado em uma organização cujo sistema de gestão de segurança da informação é certificado e está em conformidade com a NBR ISO/IEC 27001 ou Sistema de Gestão de segurança da informação Certificado – NBR ISO/IEC 27001. Esta declaração, porém, deve atender aos três itens citados em 18.10.

*e) É permitido o uso de símbolos ou logomarcas em panfletos e material publicitário. A organização deverá ter atenção adequada, para a não utilização da certificação de Sistemas de Gestão de Segurança da Informação SAS de maneira a prejudicar a imagem da SAS com declarações indevidas ou não autorizadas.

18.12 - A SAS, através deste regulamento, parte integrante do Contrato de Certificação exige que o cliente certificado:

a) atenda aos requisitos da SAS ao fazer referência à sua condição de certificação nos meios de comunicação, como internet, folhetos ou propaganda, ou outros documentos.

b) não faça ou permita qualquer declaração que induza a erro em relação à sua certificação,

c) não use ou permita o uso de um documento de certificação ou de qualquer parte dele, de maneira que induza a erro,

d) em caso de cancelamento da sua certificação, interrompa o uso de todo material publicitário que faça referência à certificação, conforme orientações da SAS,

e) altere todo material publicitário quando o escopo da certificação tiver sido reduzido,

f) não permita que a referência à certificação de seu sistema de gestão seja usada de tal forma que implique que a SAS certifique um produto (incluindo serviço) ou processo,

g) não dê a entender que a certificação aplica-se a atividades e locais fora do escopo de certificação, e

h) não use sua certificação de tal maneira que possa comprometer a reputação da SAS e/ou o sistema de certificação e perder a confiança pública.

18.13 - A SAS controla através do Relatório de Auditoria - FORM. 11.1, quanto à propriedade, uso e exibição das marcas e logomarcas da certificação de Sistemas de Gestão de Segurança da Informação SAS.

19 - Marca SAS de Organização Certificada (Desenhos, Logomarcas e Modelos)

São as seguintes as Marcas SAS de Organização Certificada:

A) Certificado NBR ISO/IEC 27001:2022

19.1 - O tamanho mínimo para apresentação da Marca SAS de Organização Certificada aplicável é de 2,5 cm de altura, de forma a garantir a perfeita legibilidade nas mídias impressas.

19.2 - As tonalidades das cores da Marca SAS de Organização Certificada aplicável deverão ser mantidas ou deverão ser aplicadas em uma só cor (PRETO).

19.3 - A SAS deverá fornecer às organizações que possuem o Certificado de Sistemas de Gestão de Segurança da Informação SAS, por meio eletrônico, um modelo da Marca aplicável.

19.4 - Caso o certificado da organização seja acreditado pela Coordenação Geral de Acreditação – Cgcre (o que é identificado na Proposta técnica–comercia/Contrato de certificação aceita pela organização e pelo símbolo de acreditação no rodapé do Certificado), esta deverá utilizar uma das Marcas SAS de Organização Certificada aplicáveis apresentadas acima.

19.5 - As organizações não poderão utilizar a logomarca institucional do INMETRO ou o símbolo de acreditação Cgcre para identificar a certificação do Sistema de Gestão de segurança da informação NBR ISO/IEC 27001.

19.6 - As dúvidas que porventura surgirem referentes à divulgação da certificação da organização, deverão ser encaminhadas à Diretoria de Certificação da SAS para apresentação de solução.

20 - Responsabilidade

A concessão do Certificado de Sistemas de Gestão de Segurança da Informação e do direito de uso da Marca SAS de Organização Certificada não substituem, em caso algum, a garantia que corresponde à organização nos termos da Lei.

20.1 - O uso abusivo do Certificado e da Marca SAS de Organização Certificada pela organização ou por terceiros, poderá acarretar a tomada de ações pela SAS podendo incluir pedidos para correção e ação corretiva, as sanções previstas no item 14.5.2 deste Regulamento, publicação da transgressão e, se necessário, ação legal.

20.2 - Será considerado uso abusivo do Certificado e da Marca SAS de Organização Certificada o não cumprimento do disposto nos itens 18 e 19 deste Regulamento, bem como as referências enganosas ao Sistema de Certificação, ou uso incorreto do Certificado e da Marca na internet, folhetos ou propaganda, outros documentos, no próprio produto e etc.

20.3 - A SAS considera como falta grave aquela cometida por uma organização certificada que tenha realizado uma ou mais das seguintes condutas o descrito no item 14.5 deste Regulamento.

21 - Confidencialidade

A SAS, por meio de acordos legais e vigentes, possuirá política e mecanismos para salvaguardar a confidencialidade das informações obtidas ou geradas durante a realização de atividades de certificação em todos os níveis da sua estrutura, inclusive Conselho de Certificação e organismos externos ou pessoas atuando em seu nome.

21.1 - As informações consideradas pela SAS como de acesso confidencial são documentos/informações dos clientes (organizações certificadas ou em processo de certificação) ou pessoa em particular obtidas em função das atividades de certificação, salvo aquelas que o cliente tornou acessíveis ao público.

21.2 - As informações sobre o cliente provenientes de outras fontes que não o próprio cliente (reclamante, regulamentadores ou outros aplicáveis) também são consideradas pela SAS como de acesso confidencial, em coerência com sua política.

21.3 - Respeitado o disposto neste item ou por força de Lei, as informações sobre um cliente ou pessoa em particular não deverão ser divulgadas a terceiros sem o prévio consentimento, por escrito, da organização em questão ou pessoa envolvida. Caso a SAS seja obrigada por Lei a revelar informações de acesso confidencial a terceiros, o cliente ou pessoa envolvida, a menos se regulamentado por Lei, deverá ser notificado antecipadamente das informações fornecidas.

21.4 - O pessoal da SAS, inclusive quaisquer membros do Conselho de Certificação, fornecedores, pessoal de organismos externos ou pessoas externas atuando em nome da SAS, deverão manter confidenciais todas as informações obtidas ou geradas durante a realização das atividades pertinentes. A este propósito, são assinados os Códigos de Ética e os Contratos firmados deverão conter cláusula que estabeleça o compromisso com a confidencialidade das informações objeto destes.

21.5 - A SAS não permite à equipe auditora proceder fotos / capturas de telas de informação documentada ou outro tipo de evidências sem a autorização da organização.

21.6 - Os Critérios de Confidencialidade de uma auditoria, incluindo segurança e proteção de dados, são de conhecimento da equipe auditora.

21.7 - A SAS possui disponíveis e usa equipamentos e instalações que garantem a segurança no tratamento das informações de acesso confidenciais (documentos, registros e outros aplicáveis).

21.7.1 - Os documentos de acesso de confidencialidade diferentes, quando conservados em uma mesma pasta ou arquivo, deverão ser tratados como de acesso confidencial.

21.7.2 - O acesso a computadores, em cuja memória estejam arquivadas informações confidenciais, deverá ser protegido por senhas.

21.7.3 - A critério da SAS e quando necessário, os documentos confidenciais serão enviados através de carta registrada ou através de portador/mensageiros contra recibo ou protocolo.

21.7.4 - A confidencialidade das informações é de responsabilidade do Diretor de Certificação e só terão acesso às mesmas, os Diretores e o pessoal administrativo da SAS.

21.8 - Quando informações confidenciais forem divulgadas a outros organismos (organismo de acreditação, grupo de acordo de um esquema de avaliação entre pares e outros aplicáveis), a SAS deverá informar o cliente dessa ação.

21.9 - Caso o certificado da organização seja acreditado pela Coordenação Geral de Acreditação - Cgcre (o que é identificado pelo símbolo de acreditação no rodapé do certificado) é assegurado a 21.10 - Cgcre o acesso a todas as informações pertinentes aos processos de certificação desenvolvidos no âmbito da acreditação da SAS.

21.11 - Os Critérios de Confidencialidade de uma auditoria, incluindo segurança e proteção de dados, são de conhecimento da equipe auditora.

21.12 - A SAS possui disponíveis e usa equipamentos e instalações que garantem a segurança no tratamento das informações de acesso confidenciais (documentos, registros e outros aplicáveis).

21.12 - Os documentos de acesso de confidencialidade diferentes, quando conservados em uma mesma pasta ou arquivo, deverão ser tratados como de acesso confidencial.

21.13 - O acesso a computadores, em cuja memória estejam arquivadas informações confidenciais, deverá ser protegido por senhas.

21.14 - A critério da SAS e quando necessário, os documentos confidenciais serão enviados através de carta registrada ou através de portador/mensageiros contra recibo ou protocolo.

21.15 - A confidencialidade das informações é de responsabilidade do Diretor de Certificação e só terão acesso às mesmas, os Diretores e o pessoal administrativo da SAS.

8.4.18 - Quando informações confidenciais forem divulgadas a outros organismos (organismo de acreditação, grupo de acordo de um esquema de avaliação entre pares e outros aplicáveis), a SAS deverá informar o cliente dessa ação.

21.16 - Caso o certificado da organização seja acreditado pela Coordenação Geral de Acreditação - Cgcre (o que é identificado pelo símbolo de acreditação no rodapé do certificado) é assegurado a Cgcre o acesso a todas as informações pertinentes aos processos de certificação desenvolvidos no âmbito da acreditação da SAS.

21.17 - Acesso a registros organizacionais

Antes da auditoria de certificação, a SAS Certificadora solicita ao cliente que relate se alguma informação relacionada ao SGSI (como registros do SGSI ou informações sobre o projeto e a eficácia dos controles) não puder ser disponibilizada para revisão pela equipe de auditoria porque contém informações confidenciais ou sensíveis. A SAS Certificadora determina se o SGSI pode ser adequadamente auditado na ausência de tais informações.

Se a SAS Certificadora concluir que não é possível auditar adequadamente o SGSI sem revisar as informações confidenciais ou sensíveis identificadas, ela informar ao cliente que a auditoria de certificação não pode ocorrer até que os acordos de acesso apropriados sejam concedidos.

22 - Notificação de alterações pela SAS

O presente Regulamento poderá ser alterado por iniciativa da SAS.

A SAS disponibiliza o presente regulamento em seu website, devendo a organização monitorar as alterações realizadas através da consulta periódica ao mesmo e durante as auditorias subsequentes será verificado se cada cliente certificado atende aos novos requisitos.

23 - Disposições finais

Os casos omissos e dúvidas suscitadas quanto à aplicação desta Publicação serão dirimidos pelo Diretor de Certificação ou pelo Conselho de Certificação da SAS.