



**PROCEDIMENTO GERAL DE CERTIFICAÇÃO**

<b>ELABORADO POR:</b>	<b>REVISADO POR:</b>	<b>APROVADO POR:</b>
Administração (Rosana Glória dos Santos)	Administrativo (Edson Alves)	Diretoria de Tecnologia (Edinei Pires Filho)

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   2 DE 17</b>
		18/11/2022	

VERSÃO	DATA	ATUALIZAÇÃO
1.0	28/12/2022	Aprovação e Emissão Inicial

## 1. Objetivo

Este procedimento tem como objetivo direcionar as informações necessárias para colaboradores, clientes e demais partes interessadas a respeito das regras internas relativas ao processo de Certificação da Access Security.

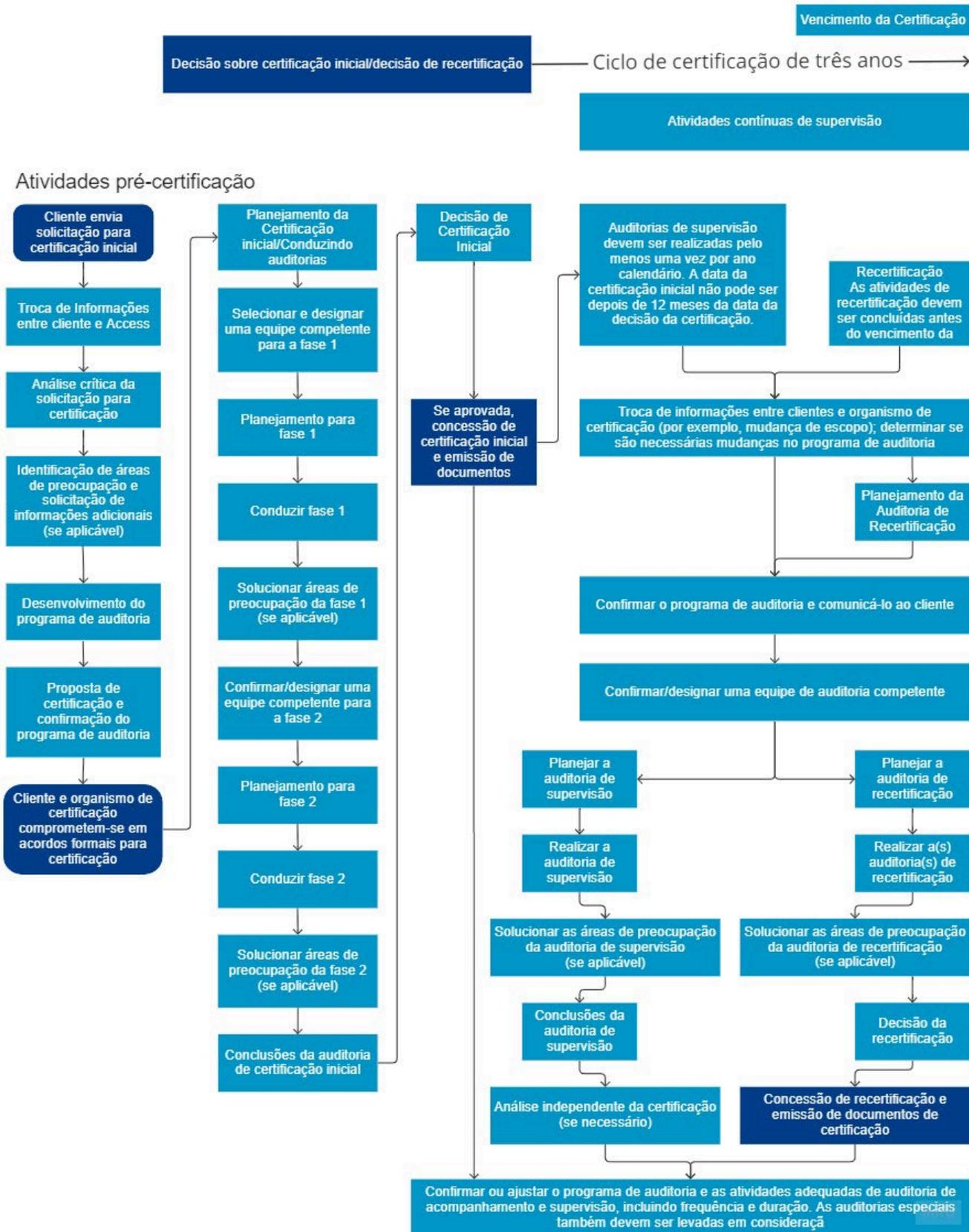
## 2. Referências

Na construção desse documento foram utilizadas como referência os seguintes documentos:

- ABNT NBR ISO/IEC 17021-1 – Avaliação da conformidade – Requisitos para organismos que fornecem Auditorias e certificação de sistemas de gestão;
- ABNT NBR ISO 9001 – Requisitos Sistema de Gestão da Qualidade;
- NIE-CGCRE-009 – Uso da Marca, do Símbolo e de Referência à Acreditação;
- NIT-DICOR-008: Critérios de acreditação para organismos de certificação de sistemas de gestão;
- NIT-DICOR-054 – Documentos mandatórios do IAF para aplicação da ABNT NBR ISO/IEC 17021/1;
- Portaria nº 274, de 13 de junho de 2014 – Regulamento para uso das marcas, dos símbolos, dos selos e das etiquetas do Inmetro.



### 3. Fluxo de Atividades



	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   4 DE 17</b>
		18/11/2022	

#### 4. Contato com o cliente e tomada de informações

Antes de iniciar qualquer atividade de certificação, a Access Security entra em contato com o possível cliente, coleta as informações necessárias, através do envio e preenchimento do documento “PNC-001 – Análise de Ambiente”. Dentre as informações a serem coletadas, a Access poderá solicitar dados para entender o escopo desejado da certificação, 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 pertinentes, identificação de todos os processos terceirizados usados pela organização que afetarão a conformidade com os requisitos, as normas ou outros requisitos para os quais a solicitante busca certificação e se consultoria relativa ao sistema de gestão a ser certificado foi fornecida e, se sim, quem forneceu.

Após o recebimento das informações por parte do cliente, na ausência de informações e/ou geração de dúvida de informação, o setor comercial entra em contato com o representante do cliente para tratamento da informação.

De posse da informação completa, a Access Security realiza uma análise crítica das informações e registra tal análise em um sistema interno de chamados, destinado para análise do setor técnico. Nesta análise deve conter as informações que assegure que as informações sobre a organização solicitante e seu sistema de gestão sejam suficientes para desenvolver um programa de auditoria, que qualquer diferença reconhecida de interpretação entre a Access e a organização solicitante seja resolvida e que o organismo de certificação tenha competência e capacidade para executar a atividade de certificação.

Em caso de aprovação e parecer do auditor deve ser elaborada uma Proposta Comercial ao Cliente “PNC-002 – Proposta Comercial” informando os processos e se aplicável, os requisitos normativos para certificação. Caso opte por não elaborar uma Proposta Comercial ao cliente, o motivo deve ser claramente relatado ao mesmo. Quando da aprovação da Proposta Comercial pelo cliente, é elaborado um Contrato que regerá as condições sobre as taxas cobradas para solicitação, certificação inicial e manutenção “PNC-003 – Contrato de Prestação de Serviços”, com um código único para identificação do cliente, podendo estas serem alteradas mediante comunicação prévia da Access Security e acordo entre as partes.

#### 5. Programa de Auditorias

A Access Security, estabelece conforme descrito abaixo um programa de auditoria para cada ciclo de certificação.

O programa de auditoria deve ser construído após a assinatura de contrato e discussão com o cliente e para tal são utilizadas as informações providas da análise crítica de contrato realizada através do sistema interno de chamados da Access Security.

Este programa deve conter a previsão da realização das auditorias no ciclo, que normalmente contempla uma auditoria de certificação inicial dividida em 2 fases, duas auditorias de manutenção e uma de recertificação, que na verdade representa o ponto de reinício do ciclo.

O programa do ciclo de auditoria e cada planejamento dos eventos de auditoria devem ter seus objetivos de auditoria determinados em conjunto com os clientes. O escopo e os critérios de auditoria, incluído quaisquer alterações, devem ser estabelecidos pela Access Security após discussão com o cliente. O monitoramento da evolução do programa de auditoria incluindo a evidência de realização das etapas e dos itens auditados, é realizado através do formulário “PCA-001 – Programa de Ciclo de Auditoria”.

O programa de ciclo de auditoria deve ser apresentado e as datas de auditoria devem ser previamente acordadas com a organização do cliente, o plano também deve descrever o que deve ser realizado pela auditoria e devem incluir a determinação da conformidade do sistema de gestão do cliente, ou de parte desse sistema, com os critérios de auditoria; determinação da capacidade do sistema de gestão para assegurar que o cliente atenda aos requisitos estatutários, regulamentares e contratuais, determinação da eficácia do sistema de gestão para assegurar que o cliente pode

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   5 DE 17</b>
		18/11/2022	

razoavelmente esperar atender seus objetivos definidos e conforme aplicável, identificar áreas para possível melhoria no sistema de gestão.

Com o programa de auditoria definido para o ciclo, o processo operacional entra em contato com o cliente para iniciar as tratativas de agendamento das auditorias que compõe o ciclo de certificação. Com exceção das auditorias de certificação inicial e auditorias de transferência – o agendamento de cada evento (início do planejamento de auditoria) deveria ser iniciado cerca de 90 (noventa) dias antes da data de realização.

Por exemplo: Um evento de auditoria de manutenção que necessita ser realizado no mês de agosto deveria ter sua programação iniciada no mês de maio do mesmo ano.

Os eventos de planejamento de cada evento da auditoria consistem basicamente no contato com o cliente para a confirmação dos dados de certificação, bem como na confirmação da equipe auditora. Caso o cliente informe alguma modificação significativa relativa ao escopo do programa de auditoria, uma nova análise crítica deve ser realizada.

A definição dos membros da equipe auditora deve ser realizada com base nas qualificações pertinentes ao atendimento dos requisitos da auditoria (competência do auditor x escopo de auditoria). Quando a equipe for composta por apenas um auditor este deverá ser qualificado no ramo ao qual o escopo de auditoria se refere. Quando a equipe for composta por mais de um auditor, pelo menos um desses deve estar devidamente qualificado. Quando nenhum auditor da equipe tiver a qualificação necessária para o escopo, um especialista deve fornecer o suporte necessário para realização da auditoria.

Para a preparação do plano de auditoria, é importante que os documentos sejam apropriados aos objetivos e escopo da auditoria, devendo haver referências no mínimo aos seguintes itens:

- a) os objetivos da auditoria;
- b) os critérios da auditoria;
- c) o escopo da auditoria, incluindo a identificação das unidades organizacionais e funcionais ou dos processos a serem auditados;
- d) as datas e lugares onde as atividades de auditoria no local serão realizadas, incluindo visitas a sites temporários e atividades de auditoria remota, conforme apropriado;
- e) a duração esperada das atividades da auditoria no local;
- f) as funções e responsabilidades dos membros da equipe auditora e das pessoas acompanhantes, como observadores e intérpretes.

**Nota<sup>1</sup>:** O papel dos especialistas técnicos durante uma auditoria deve ser acordado entre o organismo de certificação e o cliente antes da condução da auditoria. Um especialista técnico não pode atuar como auditor na equipe auditora. Os especialistas técnicos devem estar acompanhados por um auditor.

**Nota<sup>2</sup>:** Os auditores e especialistas técnicos devem estar bem-informados sobre os processos de auditoria, requisitos de certificação e outros requisitos pertinentes. Os envolvidos no processo de certificação devem ter acesso a um conjunto atualizado de procedimentos documentados, contendo instruções da auditoria e todas as informações pertinentes sobre a atividade de Certificação.

Em equipes com mais de um auditor, o processo operacional definirá um dos membros como Auditor Líder. Este auditor deve ser o responsável pela elaboração do plano de auditoria “PCA-002 – Planejamento de Auditoria”, com base nas informações solicitadas ao cliente, além de ser responsável pela condução das atividades nas instalações do cliente, bem como da elaboração dos documentos e registros determinados como necessários para a tomada de decisão de certificação.

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   6 DE 17</b>
		18/11/2022	

A presença e a justificativa para observadores durante uma atividade de auditoria devem ser acordadas junto ao cliente antes da realização da auditoria. A equipe auditora deve assegurar que os observadores não influenciem ou interfiram indevidamente no processo ou resultado da auditoria.

A equipe definida, ou parte dela, pode ser recusada pela empresa, desde que uma justificativa seja apresentada formalmente. Neste caso a Access Security irá realizar as devidas substituições e apresentar opções ao cliente.

O plano de auditoria “PCA-002 – Planejamento de Auditoria”, deve ser enviado ao cliente com antecedência, para que o cliente tenha tempo suficiente para a comunicação aos processos internos e, quando necessário, solicitar alterações. Após o recebimento do plano, caso o cliente não entre em contato para discutir o conteúdo do mesmo em até 5 (cinco) dias úteis, considera-se que o mesmo foi aprovado. De qualquer maneira, na reunião de abertura o auditor líder sempre deve confirmar se o cliente recebeu o plano de auditoria e se existem solicitações para alterações por parte do cliente.

**Nota<sup>3</sup>:** A Access Security, no Planejamento de Auditoria, deverá informar os requisitos do organismo de certificação para que os clientes atendam aos requisitos de certificação; tomem todas as medidas Necessárias para a realização das auditorias, incluindo as disposições para análise da documentação e o acesso a todos os processos e áreas, registros e pessoal para fins de certificação inicial, supervisão, recertificação e solução das reclamações; e tomem providências, quando aplicável, para acomodar a presença de observadores (por exemplo, auditores de acreditação ou auditores em treinamento).

## 5.1. Reunião de Abertura

A Access Security realizará junto com o organismo solicitante uma reunião formal de abertura com a Alta Direção do cliente e, quando apropriado, com o responsável pelas funções ou processos a serem auditados. O propósito da reunião de abertura, geralmente conduzida pelo auditor-líder, é fornecer uma breve explicação de como as atividades de auditoria serão realizadas. O grau de detalhes deve ser coerente com a familiaridade do cliente com o processo de auditoria e deve considerar, no mínimo, a apresentação dos participantes, incluindo resumo de suas funções, a confirmação do escopo de certificação, aprovação do plano de auditoria, forma de comunicação entre as partes, confirmação de assuntos relativos a confidencialidade, confirmação de procedimentos pertinentes a segurança do trabalho, confirmação da disponibilidade, funções e identidades dos guias e observadores e informações sobre o processo geral de certificação.

**Nota<sup>1</sup>:** Nas reuniões de abertura, o cliente pode solicitar alterações no plano de auditoria quanto a horário, data e até processos a serem auditados, desde que tais processos não façam parte daqueles considerados como mínimos obrigatórios em todas as fases do ciclo de auditoria e que a não realização da auditoria nesse processo não cause riscos significativos ao processo de auditoria.

## 6. Processo de Auditoria

A Access Security realiza suas auditorias utilizando como critério:

- i) Os requisitos estabelecidos na(s) norma(s) que são objetivo do programa de auditoria solicitado pelo cliente;
- ii) O escopo de certificação determinado pelo cliente, realizando a validação do mesmo pela equipe auditora;
- iii) Os documentos internos publicados pelo cliente;
- iv) Os documentos externos adicionais reconhecidamente ligados ao escopo do sistema de gestão adotado pelo cliente.

As auditorias são realizadas de forma padronizada, utilizando-se de métodos de amostragem e sempre com foco nos processos estabelecidos pelos clientes, visando a obtenção de uma avaliação consistente e coerente, em busca das conformidades do Sistema de Gestão, mantendo a credibilidade e imparcialidade do processo de auditoria. Durante as auditorias, cada auditor deve ser acompanhado por um guia, a menos se acordado de outra forma pelo auditor líder e pelo

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   7 DE 17</b>
		18/11/2022	

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.

O escopo de auditoria deve descrever a abrangência e os limites da auditoria, como as plantas, unidades organizacionais, atividades e processos a serem auditados. Quando o processo inicial ou de recertificação consistir em mais de uma auditoria (por exemplo, abrangendo diferentes plantas), o escopo de uma auditoria individual não pode abranger o escopo completo da certificação, mas o total de auditorias deve ser coerente com o escopo constante no documento de certificação.

Quando a certificação se referir à múltiplas normas de gestão, o planejamento para a auditoria deve assegurar uma auditoria adequada no local, a fim de propiciar confiança na certificação.

A Access Security estabelece um planejamento de auditoria para cada evento dentro do ciclo de auditorias. Estes planos devem servir como base para acordo em relação à realização e programação das atividades de auditoria.

O Sistema de Gestão é uma propriedade do cliente, que precisa ser avaliado, mas, sobretudo, suas características devem ser respeitadas. O contexto atual da empresa deve ser levado em consideração, desde que sejam preservadas as exigências das normas aplicáveis.

É através do processo de auditoria que a Access Security inicia a coleta de informações sobre o sistema de gestão dos clientes, e na categoria de Organismo de Avaliação de Conformidade indica, após análise técnica e formal dos resultados demonstrados pela equipe auditora, a decisão quanto a concessão, renovação, suspensão, restauração após suspensão, ou ainda cancelamento da certificação.

## **6.1. Fases do Processo de Auditoria**

### **6.1.1. Certificação Inicial**

A fase de certificação inicial de um sistema de gestão deve ser realizada em duas fases distintas, sendo a Fase 1 uma análise básica do nível de implementação do sistema de gestão do cliente e a Fase 2 uma análise completa do sistema de gestão, onde são auditados todos os requisitos normativos. As fases 1 e 2 de auditoria são realizadas de forma independente e são registradas nos respectivos documentos necessários para a tomada de conclusão sobre os processos de auditoria.

**Nota<sup>1</sup>:** 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.

#### **a) Fase 1**

A fase 1 de auditoria deve preferencialmente ser realizada nas instalações dos clientes, porém, fatores intrínsecos ou extrínsecos ao plano de auditoria (deslocamento excessivo ou desproporcional ao volume de auditoria, acesso dificultoso às instalações do cliente, causas naturais etc.) devidamente analisados e registrados pela Access Security podem suscitar em uma auditoria de análise de documentos realizada a distância. A justificativa pela escolha do local de uma realização da Auditoria fase 1 será registrada na Análise Crítica instruída no sistema de chamados interno.

Possíveis Pontos de Melhoria gerados nas auditorias são descritos formalmente aos clientes, contudo, não necessitam a elaboração de ações corretivas.

Os objetivos da fase 1 de auditoria são:

- a) Análise crítica do sistema de gestão do cliente e da informação documentada pertinente;
- b) Avaliação das condições específicas da planta do escopo do cliente e discussão com o pessoal do cliente, a fim de determinar o grau de preparação para a fase 2;

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   8 DE 17</b>
		18/11/2022	

- c) Análise crítica da 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;
- d) Obtenção das informações necessárias em relação ao escopo do sistema de gestão. Incluindo a(s) planta(s) do cliente, processos, equipamentos utilizados, níveis dos controles estabelecidos (particularmente no caso de clientes multisites), requisitos estatutários e regulatórios aplicáveis;
- e) Análise crítica da alocação de recursos para a fase 2 e acordo com o cliente dos detalhes para fase 2;
- f) Contribuir no planejamento da fase 2, obtendo um entendimento suficiente do sistema de gestão do cliente e do seu funcionamento no local, no contexto da norma de sistema de gestão escolhida pelo cliente;
- g) Avaliação do planejamento e execução das auditorias internas e das análises críticas pela direção, e se o nível de implementação do sistema de gestão está pronto para a fase 2.

A fase 1 leva em consideração o estabelecimento da documentação necessária para a implementação da documentação, como por exemplo, objetivos, políticas, escopo de atividades, controle de processos, auditoria interna e análise crítica. Ainda leva em consideração a compreensão do cliente quanto aos requisitos aplicáveis, preparação e planejamento para realização da próxima fase de certificação.

**Nota<sup>1</sup>:** Para Sistemas Integrados de Gestão, a equipe auditora deve avaliar o nível de integração do sistema, considerando documentos, elementos e responsabilidades.

**Nota<sup>2</sup>:** Para auditoria com amostragem de *multi-site* para a auditoria do sistema de gestão de um cliente que cubra a mesma atividade em diversas localizações geográficas, o organismo de certificação deve desenvolver um programa de amostragem, a fim de assegurar uma auditoria adequada do sistema de gestão.

**Nota<sup>3</sup>:** Quando houver múltiplas plantas que não cubram a mesma atividade, amostragem não é adequada.

A auditoria fase 1 tem como resultado a avaliação da prontidão da organização para seguir com o processo de certificação, podendo ser identificadas áreas de preocupação as quais podem ser classificadas como não conformidades durante a auditoria fase 2.

Caso a equipe auditora entenda que as áreas de preocupação impedem a continuidade do processo, a Fase 2 deverá ser reavaliada, podendo ser adiada para que as ações necessárias sejam tomadas. Se as ações resultantes da auditoria Fase 1 gerarem mudanças significativas e de impacto extremo, a repetição de parte ou de toda Fase 1 deve ser avaliada.

## b) Fase 2

A fase 2 da auditoria inicial de certificação pode ser agendada antes do término da primeira fase da auditoria. Caso necessário, estas Auditorias poderão ser realizadas em conjunto, ou seja, agendadas em sequência. Isto significaria a realização da Auditoria de Fase 1 nos dias necessários segundo dimensionamento, com início da Auditoria de Fase 2, no dia seguinte ao término da primeira. Esta condição deve ser acordada com o cliente para que o mesmo possa se programar e se preparar para tais eventos.

A fase 2 da auditoria deve ser realizada integralmente nas instalações do cliente, a menos que o acesso a tais instalações cause riscos para a saúde e segurança dos auditores e auditados (por exemplo, casos de pandemia, acidentes e/ou eventos naturais) e/ou seja inviável tecnicamente (por exemplo, escopo totalmente automatizado com controles a distância). Caso a fase 2 necessite ser realizada de forma remota, uma análise crítica dos riscos da realização dessa auditoria será realizada e documentada como forma de registro.

A fase 2 da auditoria de certificação inicial deve ser realizada de forma a abranger todo o sistema de gestão do cliente (todos os processos e requisitos considerados como aplicáveis pelo cliente).

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   9 DE 17</b>
		18/11/2022	

Os objetivos da fase 2 da auditoria consistem em avaliar a implementação, incluindo eficácia, do sistema de gestão do cliente. Ela deve incluir a auditoria de no mínimo o seguinte:

- a) Informações e evidências sobre a conformidade com todos os requisitos da norma aplicável do sistema de gestão determinado pelo cliente;
- b) Monitoramento, medições, comunicação e análise crítica do desempenho em relação aos principais objetivos e metas de desempenho (coerente com as expectativas na norma aplicável ao sistema de gestão ou outro documento normativo);
- c) A capacidade e o desempenho do sistema de gestão do cliente em relação ao atendimento dos requisitos estatutários, regulatórios e contratuais;
- d) Controle operacional dos processos do cliente;
- e) Auditoria interna e análise crítica pela direção;
- f) Responsabilidade da direção pelas políticas do cliente.

### 6.1.2. Manutenção da Certificação

Para manutenção da Certificação do Sistema de Gestão, são realizadas auditorias de supervisão nas instalações do cliente, a menos que o acesso a tais instalações cause riscos para a saúde dos auditores e auditados (p.e: casos de pandemia, acidentes e/ou eventos naturais) e/ou seja inviável tecnicamente (p.e: escopo totalmente automatizado com controles a distância). Caso a auditoria de manutenção necessite ser realizada de forma remota, uma análise crítica dos riscos da realização dessa auditoria será realizada e documentada como forma de registro.

As auditorias de manutenção devem ser planejadas de modo a ocorrerem no mínimo duas vezes após a decisão de certificação, preferencialmente uma vez ao ano, exceto em anos de recertificação, sendo o primeiro evento de manutenção obrigatoriamente no prazo máximo de 12 meses após a decisão de certificação e o segundo evento de manutenção ocorrendo em até 24 meses após a decisão de certificação com tolerância máxima de 60 dias após esse limite devidamente justificada pelo cliente.

As auditorias de manutenção não são necessariamente auditorias completas do sistema de gestão do cliente. Os processos que compõem o sistema de gestão do cliente podem ser alternados entre os eventos de manutenção, contudo, em cada evento de manutenção, deve ser obrigatoriamente verificado:

- a) A realização das auditorias internas e análise crítica pela direção;
- b) Uma análise crítica das ações corretivas para não conformidades identificadas na auditoria anterior;
- c) Gestão das reclamações, notificações e/ou autuações das partes interessadas;
- d) Eficácia do sistema de gestão com respeito ao atingimento 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 crítica de quaisquer mudanças;
- h) Uso de marcas e/ou quaisquer outras referências à certificação.

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

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   10 DE 17</b>
		18/11/2022	

Independentemente do envolvimento da autoridade reguladora competente, uma auditoria extraordinária pode ser necessária caso a Access Security tome ciência de violações graves a regulamentações e conformidade. Caso seja necessária a execução de uma auditoria extraordinária a Access Security irá documentar o resultado em um relatório final de auditoria.

### 6.1.3 Recertificação

Antes do vencimento do certificado uma auditoria de recertificação deve ser realizada e executada nas instalações do cliente, a menos que o acesso a tais instalações cause riscos para a saúde e segurança dos auditores e auditados (p.e: casos de pandemia, acidentes e/ou eventos naturais) e/ou seja inviável tecnicamente (p.e escopo totalmente automatizado com controles à distância). Caso a fase 2 necessite ser realizada de forma remota, uma análise crítica dos riscos da realização dessa auditoria será realizada e documentada como forma de registro.

Esta auditoria deve ser planejada de modo que exista tempo hábil para a renovação oportuna antes da data de expiração do certificado emitido e válido para o ciclo de auditoria.

Esta auditoria de recertificação tem por finalidade confirmar a conformidade e a eficácia contínua do sistema de gestão, assim como a contínua relevância e aplicabilidade ao escopo de certificação. A auditoria de recertificação deve ser realizada de forma completa sobre o sistema de gestão e deve abordar:

- a) A eficácia de todo o sistema de gestão, considerando mudanças internas e externas e sua relevância e aplicabilidades contínuas ao escopo de certificação;
- b) Comprometimento demonstrado para manter a eficácia e melhoria do sistema de gestão, a fim de melhorar seu desempenho global;
- c) A eficácia do sistema de gestão em relação a atingir os objetivos do cliente certificado e os resultados esperados do(s) respectivo(s) sistema(s) de gestão.
- d) Análise crítica dos relatórios de auditoria de supervisão anteriores e considerar o desempenho do escopo durante o ciclo de certificação mais recentes.

Eventuais não-conformidades maiores oriundas da auditoria de recertificação deverão ter suas resoluções antes do prazo de expiração do certificado.

**Nota<sup>1</sup>:** Nas atividades de auditoria de recertificação, pode ser necessário realizar uma nova fase 1 em situações em que houver mudanças significativas no sistema de gestão, na organização ou no contexto no qual o sistema de gestão opera (por exemplo, mudanças na legislação). A decisão da realização da nova fase 1 deve ser de comum acordo entre a Access Security e o cliente.

**Nota<sup>2</sup>:** Em caso de qualquer alteração nos requisitos para certificação, a Access Security se compromete em informar devidamente os novos clientes e verificar se cada cliente já certificado atende aos requisitos.

Se as atividades de recertificação forem completadas com sucesso antes da data de expiração da certificação vigente, a data de expiração da nova certificação será baseada na data de expiração da certificação vigente, contudo a data de emissão no novo certificado será a mesma da tomada da decisão de recertificação.

Caso as atividades de recertificação não tiverem sido completadas antes do vencimento do certificado atual, incluindo a análise da implementação de ações corretivas para não conformidades maiores, a recertificação não será recomendada e a validade do certificado não será estendida. Neste caso, a certificação fica em suspensão até sua eventual restauração após a execução das atividades pendentes, que devem ser realizados em no máximo 6 (seis) meses a contar da validade da certificação. Findado o prazo de 6 (seis) meses, o certificado será considerado como cancelado e a retomada pelo cliente só poderá ocorrer mediante a realização de nova certificação inicial (fase 1 + fase 2).

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   11 DE 17</b>
		18/11/2022	

#### 6.1.4. Avaliação de Não Conformidades

Em caso de ocorrência de não-conformidades em qualquer evento de auditoria, a avaliação das não-conformidades maiores deve ser realizada no máximo 6 (seis) meses após o último dia de auditoria.

A avaliação das não-conformidades maiores pode ser realizada de forma presencial ou remota nas instalações do cliente, ficando essa decisão para o auditor líder do evento.

Para não-conformidades menores, o cliente deve documentar um plano de ação em até 30 (trinta) dias após o último dia de auditoria, porém, a avaliação da implementação das ações deve ser realizada em conjunto com o próximo evento de auditoria. O acréscimo de tempo de auditoria em função da necessidade da avaliação de não conformidades deve ser negociado com o cliente.

#### 6.1.5. Auditoria de Transferência

Em caso de auditorias de transferência de certificação, primeiramente é importante definir que somente as certificações cobertas pela acreditação de um signatário do MLA do IAF devem ser elegíveis para transferência. As organizações portadoras de certificações que não estejam cobertas por tais acreditações devem ser tratadas como novos clientes (processo de certificação novo).

Antes da realização de uma auditoria de transferência, uma análise crítica deve ser realizada através de uma análise da documentação disponibilizada pelo cliente potencial, e se for viável, pelo organismo de certificação atual (a menos que ele tenha encerrado as atividades). Essa documentação deve demonstrar a validade/autenticidade da certificação atual e a situação de não-conformidades pendentes com o organismo atual de certificação.

**Nota:** Quando não for possível se comunicar com o organismo de certificação atual, o organismo de certificação receptor deve registrar os motivos.

Tal análise crítica deve abordar:

- a) Confirmação de que as atividades certificadas do cliente estão dentro do escopo acreditado da Access Security;
- b) Os motivos pelos quais o cliente solicita a transferência;
- c) Que o site ou sites que desejam a transferência da certificação mantém uma certificação acreditada válida, em termos de autenticidade, duração e escopo de atividades cobertas pela certificação de sistema de gestão.
- d) Uma análise dos relatórios relativos ao último ciclo de auditoria – últimos 3 anos – quanto as informações, resultados, decisões e eventuais não conformidades fechadas ou pendentes.
- e) Qualquer outra documentação pertinente disponível, relacionada ao processo de certificação, isto é, anotações manuscritas, listas de verificação. Se os últimos relatórios de auditoria de certificação, recertificação ou supervisão subsequentes não forem disponibilizados ou se a auditoria de supervisão estiver atrasada, então a organização deve ser tratada como um novo cliente;
- f) Eventuais reclamações recebidas e as ações tomadas;
- g) A fase do ciclo atual de certificação;
- h) Qualquer compromisso da organização com organismos regulatórios com relação à conformidade legal.

Após concluída a análise crítica do processo de transferência, convém que, seja realizada uma visita ao cliente em potencial. O volume dessa visita deve ser estipulado na própria análise crítica. Caso seja inviável a realização desta visita, as razões devem ser plenamente justificadas e documentada.

**Nota:** Se o contato com o organismo de certificação atual for inviável ou impossível (p.e: encerramento das atividades), uma visita deve ser conduzida obrigatoriamente.

Em geral, convém que somente certificação creditada dentro dos prazos de validade seja transferida. No caso em que a certificação tenha sido concedida por um organismo de certificação que tenha encerrado suas atividades comerciais ou cuja acreditação tenha expirado, sido suspensa ou cancelada, a Access Security poderá considerar tal certificação para transferência, a seu critério. Em tais casos, antes de prosseguir com a transferência, o organismo de certificação receptor deve obter o de acordo do organismo de acreditação, cuja marca pretende colocar no certificado.

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   12 DE 17</b>
		18/11/2022	

Certificação que se sabe de antemão que tenha sido suspensa ou com ameaça de suspensão não deve ser aceita para transferência. Se a Access Security não puder verificar o estado da certificação com o organismo de certificação atual, deverá solicitar à organização que confirme que o certificado não está suspenso ou sob ameaça de suspensão. Caso existam as não-conformidades pendentes com o organismo de certificação atual, a Access Security realizará com o cliente em potencial o fechamento das mesmas.

Após o encerramento do processo de transferência, o ciclo de auditorias segue o mesmo regime ora executado com o organismo de certificação anterior. Por exemplo: Se o ciclo de auditorias estabelecia que a próxima auditoria seria um evento de recertificação, será realizada a 1ª auditoria de manutenção e assim por diante.

Nos casos em que a análise crítica documental somada a visita nas instalações do cliente ainda trouxer dúvidas sobre a adequação da certificação atual, a Access Security, mediante explicação e justificativa ao potencial cliente, irá iniciar um novo processo de certificação ou conduzirá uma auditoria especial que se concentre em áreas com problemas identificados.

#### **6.1.6. Auditorias Especiais**

##### a) Alteração de escopo

O cliente pode solicitar a qualquer tempo a análise crítica sobre alterações demandadas no escopo de auditoria. As alterações podem ser sobre:

- Os dados relativos à empresa (CNPJ, Nome Empresarial, Nome Fantasia, Endereço etc.);
- A área do escopo;
- A implementação ou exclusão de processos, produtos, turnos e atividades;
- A inclusão e/ou exclusão de requisitos da norma;
- Quantidade significativa no número de pessoas abrangidas pelo escopo de certificação;
- A frequência das visitas de acompanhamento (anual para semestral e vice-versa);
- Integração ou desintegração de sistemas de gestão.

Após a comunicação por parte do cliente, deve ser realizada uma análise crítica, incluindo sobre os riscos associados, e decidido quais as atividades necessárias para a verificação dessas alterações, sendo que isto deve ser realizado através de um evento de auditoria, que pode ser o próximo evento de manutenção, incluindo tempo adicional se necessário.

A análise das mudanças comunicadas pelos clientes pode ser realizada nas instalações do próprio, remotamente ou ainda de forma documental, sempre com base na análise crítica.

Quando a decisão de verificação determinar que uma auditoria especial seja realizada, a mesma deve ser programada e planejada adequadamente junto ao cliente, gerando os efetivos registros necessários para a comprovação da realização da mesma, incluindo a reemissão de certificado.

##### b) Auditorias sem aviso ou com pouca antecedência

Quando necessário, a critério da Access Security, uma auditoria sem aviso prévio ou avisada com pouca antecedência será realizada para a investigação de reclamações, uso inadequado de marcas da Access Security ou do órgão acreditador, ou ainda para análise de mudanças significativas ou como acompanhamento em clientes suspensos.

##### c) Auditorias de fechamento de não conformidade

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   13 DE 17</b>
		18/11/2022	

Em casos em que seja necessária a realização de uma Auditoria de Fechamento de Não conformidade Maiores, esta deve ser programada e planejada adequadamente junto ao cliente, gerando os efetivos registros necessários para a comprovação da realização da mesma. O tempo demandado para esse tipo de auditoria não é o padrão de realização das auditorias de certificação ou supervisão, sendo que será considerado conforme necessidade do evento, múltiplos de 0,5 AD (Auditor/Dia), sendo o mínimo 0,5 AD. Nestas auditorias de fechamento de não conformidade devem ser verificadas as causas das não conformidades e a eficácia das ações corretivas.

## 6.2. Comunicação das tarefas da equipe auditora

As tarefas atribuídas à equipe auditora devem ser definidas e devem determinar que a equipe auditora:

- a) examine e verifique a estrutura, políticas, processos, procedimentos, registros e documentos relacionados do cliente pertinentes à norma do sistema de gestão;
- b) confirme se esses itens atendem a todos os requisitos pertinentes ao escopo pretendido de certificação;
- c) confirme se os processos e procedimentos estão estabelecidos, implementados e mantidos com eficácia, a fim de servir de base para a confiança no sistema de gestão do cliente;
- d) comunique ao cliente, para sua ação, quaisquer incoerências entre a política, objetivos e metas do cliente.

## 7. Emissão do Relatório de Auditoria

Após a execução de cada evento de auditoria, o auditor líder do processo de auditoria deve emitir um relatório que deve ser preciso, claro e conciso, contendo as evidências necessárias para a comprovação da realização da auditoria. O auditor-líder é o profissional responsável pelo conteúdo e veracidade do relatório. Sob a responsabilidade do auditor-líder, deve ocorrer uma reunião de encerramento onde serão analisadas criticamente as constatações da auditoria, classificação das não-conformidades e conclusão de auditoria.

Além de conter os resultados que serão considerados para possibilitar uma tomada de decisão fundamentada para o estabelecimento do status da certificação (emissão, manutenção, recertificação, suspensão ou ainda cancelamento), o relatório de auditoria deve incluir ou se referir ao seguinte:

- a) Identificação do organismo de certificação;
- b) Nome, endereço do cliente e do representante do cliente;
- c) Tipo de auditoria;
- d) Critérios de auditoria;
- e) Objetivos da auditoria;
- f) Escopo da auditoria, incluindo a identificação das unidades organizacionais ou funcionais ou os processos auditados e o tempo de auditoria;
- g) Quaisquer desvios do plano de auditoria e suas razões;
- h) Quaisquer fatos significantes que impactem no programa de auditoria;
- i) Identificação da equipe auditora e dos eventuais acompanhantes;
- j) As datas e lugares onde as atividades da auditoria foram realizadas;
- k) Constatações da auditoria;
- l) Referência às evidências e conclusões, coerentes com os requisitos do tipo de auditoria;
- m) Mudanças significativas, se houverem, que afetem o sistema de gestão do cliente desde a realização da última auditoria;
- n) Quaisquer questões não resolvidas, se identificadas;
- o) Quando aplicável, se a auditoria foi combinada, conjunta ou integrada;

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   14 DE 17</b>
		18/11/2022	

- p) Uma declaração de esclarecimento indicando que a auditoria é baseada em um processo de amostragem da informação disponível;
- q) Uma recomendação da equipe auditora;
- r) Se o cliente auditado está controlando efetivamente o uso dos documentos de certificação e marcas, se aplicável;
- s) Verificação da eficácia das ações corretivas tomadas para não conformidades identificadas anteriormente, se aplicável.

Os critérios de auditoria devem ser usados como referência para determinação da conformidade e devem incluir os requisitos de um documento normativo definido sobre sistemas de gestão e os processos definidos e a documentação do sistema de gestão desenvolvido pelo cliente.

Adicionalmente deve conter uma declaração sobre a conformidade e a eficácia do sistema de gestão com um resumo das evidências relacionadas à capacidade do sistema de gestão em atender aos requisitos aplicáveis e resultados esperados; à auditoria interna e processo de análise crítica da direção; a uma conclusão sobre a adequação do escopo de certificação; e confirmação de que os objetivos da auditoria foram atingidos.

**Nota:** A Access Security é proprietária do relatório de auditoria, cedendo as devidas cópias ao cliente, quando necessário.

## 8. Decisões nos processos de Certificação

Após a emissão dos resultados de auditoria, realizada pelo auditor-líder, através dos relatórios de auditoria e demais documentos necessários, uma pessoa qualificada e independente do processo em questão faz a avaliação técnica de conteúdo (evidências, informações, análise da adequação do escopo, ações corretivas para as eventuais não conformidades tratadas durante a auditoria ou pendentes de tratamento, recomendação da equipe auditora etc.) e da completude dos registros. Como resultado dessa avaliação técnica é obtida a tomada de decisão final dos processos de auditoria, onde o avaliador técnico do processo realiza uma análise crítica final e toma uma das seguintes decisões:

### a) Concessão da Certificação Inicial

Após a conclusão da fase 2 da auditoria de certificação inicial, estando os resultados e registros completos, avaliados de forma positiva e com a devida decisão tomada pelo avaliador técnico, a Access Security emitirá o certificado e fará a distribuição das cópias necessárias e suficientes dos relatórios de auditoria ao cliente auditado.

### b) Recusa da Certificação

Estando os resultados e registros completos, que demonstram a inconformidade do escopo, o avaliador técnico emite seu parecer de recusa da emissão do certificado e documenta tal decisão à diretoria da Access Security que informa o cliente auditado. As cópias necessárias e suficientes dos relatórios de auditoria são enviadas aos clientes.

Caso seja aplicável a realização de auditorias especiais, estas serão programadas para nova avaliação e, em caso de resultado positivo, será recomendada a certificação. O prazo máximo para a execução das auditorias especiais e para recomendação da certificação é de 6 (seis) meses a partir do último dia de auditoria inicial fase 2. Findado este prazo, um novo processo de certificação (fase 1 + fase 2) deve ser iniciado.

### c) Manutenção da certificação

Após as auditorias de manutenção, estando os resultados e registros completos, avaliados de forma positiva e com a devida decisão tomada pelo avaliador técnico, a Access Security registra seu parecer de manutenção do certificado e documenta tal decisão ao cliente auditado. Autoriza também a distribuição de cópias necessárias e suficientes dos relatórios de auditoria ao cliente auditado.

### d) Recertificação

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   15 DE 17</b>
		18/11/2022	

Após as auditorias de recertificação, estando os resultados e registros completos, avaliados de forma positiva e com a devida decisão tomada pelo avaliador técnico a Access Security autoriza a emissão do novo certificado. Autoriza também, a distribuição das cópias necessárias e suficientes dos relatórios de auditoria do cliente auditado.

e) Expansão do escopo

Após a execução de auditorias onde o cliente solicita a expansão do escopo, podendo ser esta uma auditoria planejada do ciclo ou uma auditoria especial, estando os resultados e registros completos, avaliados de forma positiva pelo avaliador técnico, a Access Security documenta esta decisão ao cliente e autoriza a emissão do certificado com a alteração e a distribuição das cópias necessárias e suficientes dos relatórios de auditoria ao cliente auditado.

f) Redução do escopo

Caso o cliente falhar persistentemente ou seriamente em atender aos requisitos de certificação para determinadas partes do escopo da certificação, a Access Security, através da decisão do avaliador técnico, irá reduzir o escopo de certificação do cliente para excluir as partes que não atendam aos requisitos. Qualquer redução desse tipo deve estar de acordo com os requisitos da norma usada para certificação.

g) Restauração, suspensão e cancelamento da Certificação

Após a execução de qualquer evento de auditoria, exceto na emissão da certificação inicial, onde o sistema de gestão do cliente certificado apresentar falhas persistentes no atendimento aos requisitos normativos e não apresentar a condição da conclusão de ações corretivas consistentes e eficazes, ou ainda aonde o cliente certificado não permitir a realização de auditorias de supervisão ou de recertificação nas frequências exigidas, ou ainda aonde o cliente solicitar voluntariamente, a Access Security iniciará o processo de suspensão do certificado emitido, após a decisão do avaliador técnico.

O prazo máximo para o reestabelecimento das condições normais de certificação (isenção de não conformidades maiores e/ou isenção de não conformidades menores reincidentes) e conclusivamente da restauração do certificado é de 6 meses após o último dia de auditoria ou da solicitação de suspensão pelo cliente. Após esse prazo o certificado emitido deve ser cancelado e caso seja acordado com o cliente, um novo processo de certificação deve ser iniciado.

A Access Security deve analisar criticamente as correções, causas identificadas e ações corretivas apresentadas pelo cliente referente às não-conformidades apontadas. As evidências obtidas para apoiar a solução das não conformidades devem ser registradas. O cliente deve ser informado sobre o resultado da análise crítica e verificação. O cliente deve também ser informado se uma auditoria adicional completa, uma auditoria adicional parcial ou evidência documentada (a ser confirmada durante futuras auditorias) será necessário para verificar correções e ações corretivas eficazes.

**Nota<sup>1</sup>:** O pessoal designado pelo organismo de certificação para fazer uma decisão de certificação deve estar empregado ou deve estar sobre contrato com a Access Security, tal ação não poderá em hipótese alguma ser feita por terceiros. Todas as informações referentes a decisão de certificação, incluindo informação adicional ou esclarecimentos devem ser documentadas.

**Nota<sup>2</sup>:** A Access Security, em conformidade com a ISO 17021-1:2016, deverá informar ao cliente os requisitos normativos para a certificação.

**Nota<sup>3</sup>:** O não cumprimento por parte do cliente das obrigações contidas no contrato de prestação de serviços “PNC-003 – Contrato de Prestação de Serviços” acordado entre as partes incide também na suspensão, e quando necessário, no cancelamento do certificado.

Caso o cliente certificado não permita a participação de acompanhantes da Equipe CGCRE do INMETRO nas Auditorias, em caso de solicitação do Organismo Acreditor, ou ainda não permita a realização de qualquer verificação necessária para atendimento a denúncias recebidas, o certificado será imediatamente suspenso.

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   16 DE 17</b>
		18/11/2022	

## 10. Documento de Certificação

A Access Security fornecerá, através de qualquer meio que escolha, documentos de certificação para o cliente certificado. Os documentos indicariam o seguinte:

- a) o nome e a localização geográfica de cada cliente certificado (ou a localização geográfica da sede e de quaisquer locais incluídos no escopo de uma certificação multi-site);
- b) a data efetiva da concessão, expansão ou redução do escopo da certificação, ou renovação da certificação, que não pode ser anterior à data da respectiva decisão de certificação;
- c) a data em que expira a certificação ou a data prevista para a renovação da certificação coerente com o ciclo de renovação do certificado;
- d) um código único de identificação;
- e) a norma de sistema de gestão e/ou outro documento normativo, incluindo uma indicação da situação da emissão (por exemplo, data ou número de revisão), usado para a auditoria do cliente certificado;
- f) o escopo da certificação relativo ao tipo de atividades, produtos e serviços, conforme aplicável para cada local, sem confundir nem ser ambíguo;
- g) o nome, endereço e a marca de certificação da Access Security;
- h) quaisquer outras informações requeridas pela norma e/ou outro documento normativo usado para certificação;
- i) no caso de emissão de quaisquer documentos revisados de certificação, um meio de distinguir os documentos revisados dos documentos anteriores obsoletos.

## 11. Notificação de alterações pelo cliente certificado

O cliente certificado, conforme indicado no “PNC-003 - Contrato de Prestação de Serviços” assinado pelas partes, deverá informar sem demoras à Access Security das questões que possam afetar a capacidade do sistema de gestão de continuar a atender aos requisitos da norma usada para certificação. Essas questões incluem, por exemplo, alterações relativas a:

- a) Situação legal, comercial, organizacional ou propriedade;
- b) Organização e gestão (por exemplo, pessoal-chave, como gestores, tomadores de decisão, equipe técnica etc.);
- c) Endereço de contato e locais;
- d) Escopo das operações abrangidas pelo sistema de gestão certificado;
- e) Alterações significativas no sistema de gestão e nos processos.

A Access Security tomará ações conforme apropriado.

## 12. Registros de Clientes

A Access Security manterá de forma confidencial, durante o prazo estipulado no “PNC-004 – Acordo de Confidencialidade” os registros de auditorias e de outras atividades de certificação para todos os clientes, inclusive para todas as organizações que apresentaram solicitações e para todas as organizações auditadas, certificadas ou com a certificação suspensa ou cancelada. Dentre os registros, encontram-se:

	<b>PROCEDIMENTO GERAL DE CERTIFICAÇÃO</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>
		PGC-001	1.0
		<b>APROVADA EM</b>	<b>PÁGINA   17 DE 17</b>
		18/11/2022	

- a) informações sobre a solicitação e os relatórios de auditoria inicial, de supervisão e recertificação;
- b) contrato de certificação;
- c) justificativa da metodologia usada para amostragem de sites, se aplicável;
- d) justificativa para a determinação do tempo de auditor;
- e) verificação de correção e ações corretivas;
- f) registros de reclamações e apelações, e de quaisquer correções ou ações corretivas subsequentes;
- g) deliberações e decisões de comitês, se aplicável;
- h) documentação das decisões de certificação;
- i) documentos de certificação, incluindo o escopo de certificação com relação ao produto, processo ou serviço, conforme aplicável;
- j) registros relacionados necessários para estabelecer a credibilidade da certificação, como evidência da competência de auditores e especialistas técnicos;
- k) programas de auditorias.