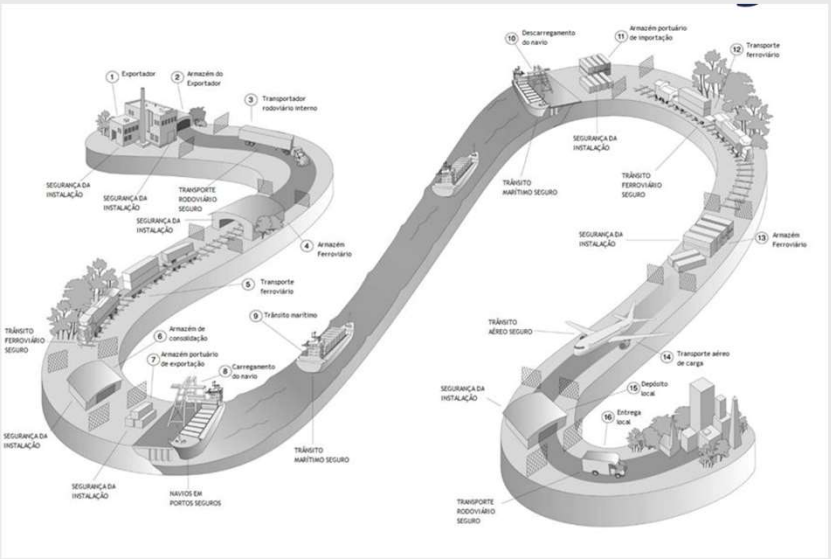

I9 Consultoria
Auditoria e Treinamentos
Projeto ISO 28000:2022
Sistema de Gestão de Segurança da Cadeia Logística

Introdução

A maioria das organizações está enfrentando uma crescente incerteza e volatilidade na segurança ambiente. Como consequência, enfrentam problemas de segurança que têm impacto nos seus objetivos, que desejam abordar sistematicamente dentro de seu sistema de gestão. Uma abordagem formal à segurança a gestão pode contribuir diretamente para a capacidade de negócios e credibilidade da organização.

No que diz respeito à cadeia de abastecimento, deve-se considerar que as cadeias de abastecimento são de natureza dinâmica. Portanto, algumas organizações que gerenciam múltiplas cadeias de abastecimento podem recorrer aos seus fornecedores para atender padrões de segurança relacionados como condição para ser incluído nessa cadeia de abastecimento, a fim de atender requisitos para gerenciamento de segurança.

Conheço minha cadeia logística e os riscos dela?



Por que gerenciar minha cadeia logística?

I9 Consultoria
Auditoria e Contabilidade

Cocaína no café: quase 800 quilos são apreendidos no Porto de Santos

Droga aprendida em São Paulo é avaliada em mais de R$ 60 milhões

Beto Souza, da CNN
14/10/2024 às 17:43 | Atualizado 14/10/2024 às 17:43

Polícia de SP encontra 800 kg de cocaína em contêiner no Porto de Santos • Reprodução / Governo de SP

Receita Federal realiza a maior apreensão do ano no Porto de Santos ao encontrar 1,2 t de cocaína em carga de sucata; VÍDEO

Droga estava escondida em um contêiner com destino ao exterior. Essa, de acordo a Receita Federal, é a maior apreensão do ano até o momento no Porto de Santos (SP).

Por g1 Santos
21/10/2024 19h39 · Atualizado há uma semana

Mais de meia tonelada de cocaína com destino à Europa é encontrada no Porto de Salvador; vídeo mostra ação dos suspeitos

Homens se esconderam em fundo falso de caminhão e levaram droga até container que já estava no porto. Sete pessoas foram presas na ação da Receita e da Polícia Federal.

Por g1 BA
18/10/2024 09h37 · Atualizado há uma semana

Quase meia tonelada de cocaína é interceptada em SC dentro de carga com destino a Hong Kong

Droga estava escondida em contêiner refrigerado com carga de pés e patas de aves congeladas.

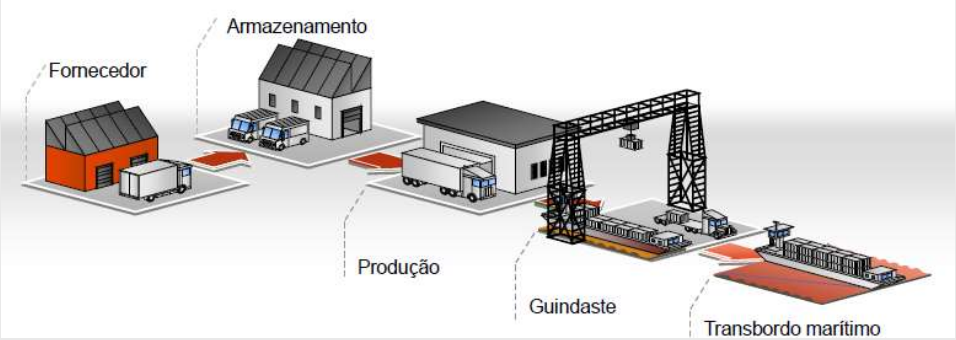
Por g1 SC
12/10/2024 12h42 · Atualizado há 2 semanas

Quase meia tonelada de cocaína é interceptada em SC dentro de carga

O objetivo da gestão da segurança dentro da organização é a criação e, em particular, a proteção do valor.

CONCEITOS PRINCIPAIS

(Segundo a NBR ISO 28000:2022)



CADEIA LOGÍSTICA

Conjunto vinculado de suprimentos e processos que se inicia a partir da obtenção de matéria-prima e se estende até a entrega de produtos e serviços ao consumidor final através das modalidades de transporte.

CONCEITOS PRINCIPAIS

(Segundo a ISO 22300:2021)

SECURITY
(Proteção)

FOCO ISO 28000

≠

SAFETY
(Segurança)

CONCEITOS PRINCIPAIS

(Segundo a ISO 22300:2021)

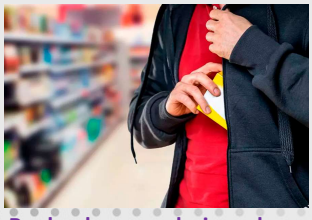
SEGURANÇA
Estado de estar livre de perigo ou ameaça.

SITUAÇÕES DE SEGURANÇA PREVENÇÃO ISO 28000

Roubo de carga/veículos

Assalto/invasão à organização

Ferimento/morte de civis



Roubo de mercadoria ou bens da organização

Interceptação/ adulteração de carga

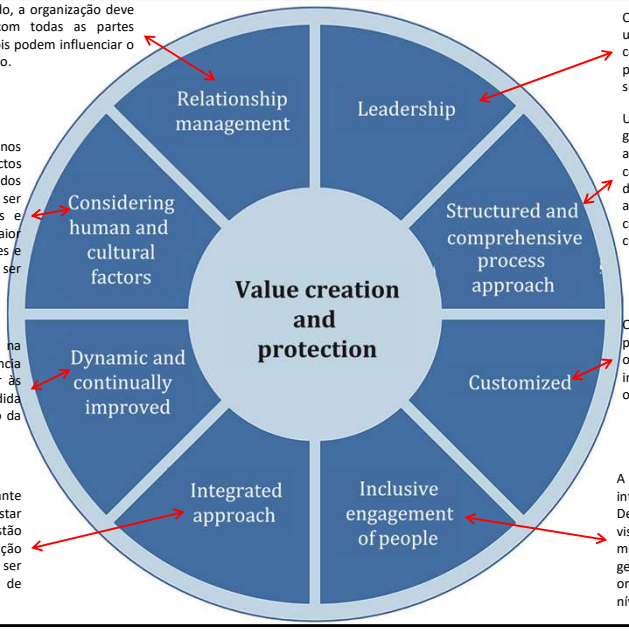
Princípios da Gestão de Segurança

Para um sucesso sustentado, a organização deve gerir as suas relações com todas as partes interessadas relevantes, pois podem influenciar o desempenho da organização.

O comportamento e a cultura humanos influenciam significativamente todos os aspectos da gestão da segurança e devem ser considerados em cada nível e estágio. As decisões devem ser baseadas na análise e avaliação de dados e informações para garantir que resultem em maior objetividade, confiança na tomada de decisões e sejam. As percepções individuais devem ser consideradas.

A organização deve ter um foco contínuo na melhoria através do aprendizado e da experiência para manter o nível de desempenho, reagir às mudanças e criar novas oportunidades à medida que o ambiente externo e o contexto interno da organização muda.

O gerenciamento da segurança é parte integrante de todas as atividades organizacionais. Deve estar integrado com todos outros sistemas de gestão da organização. A gestão de riscos da organização – seja formal, informal ou intuitiva – deve ser integrada o sistema de gerenciamento de segurança.



Os líderes de todos os níveis devem estabelecer unidade de propósito e direção. Devem criar condições para alinhar as estratégias, políticas, processos e recursos da organização para atingir seus objetivos.

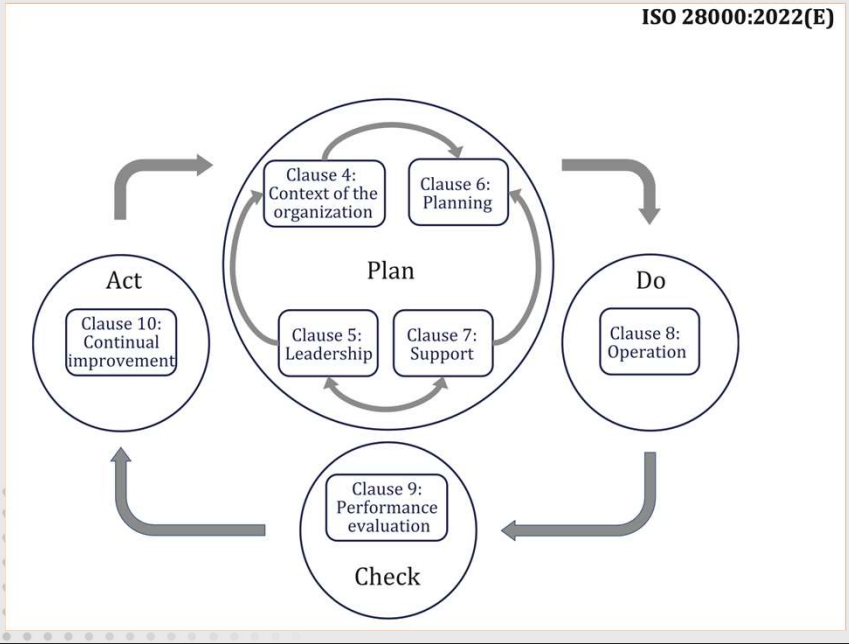
Uma abordagem estruturada e abrangente à gestão da segurança, incluindo a cadeia de abastecimento, deverá contribuir para resultados consistentes e comparáveis, que são alcançados de forma mais eficaz e eficiente quando as atividades são compreendidas e gerenciadas como processos inter-relacionados, funcionando como um conjunto coerente sistema.

O sistema de gestão de segurança deve ser personalizado e proporcional às necessidades da organização. Contexto e necessidades externas e internas. Deve estar relacionado aos seus objetivos.

A organização deve envolver as partes interessadas de forma adequada e oportuna. Deve considerar seus conhecimentos, pontos de vista e percepções de forma adequada para melhorar a conscientização e facilitar gerenciamento de segurança informado. A organização deve garantir que todos, em todos os níveis, estejam respeitando e envolvidos.

Ciclo PDCA de Gestão

ISO 28000:2022(E)



Necessidades e expectativas das partes interessadas:

A organização deve determinar:

— as partes interessadas relevantes para o sistema de gestão da segurança;

— os requisitos relevantes destas partes interessadas;

— quais destes requisitos serão abordados através do sistema de gestão da segurança.

Requisitos legais, regulatórios e outros:

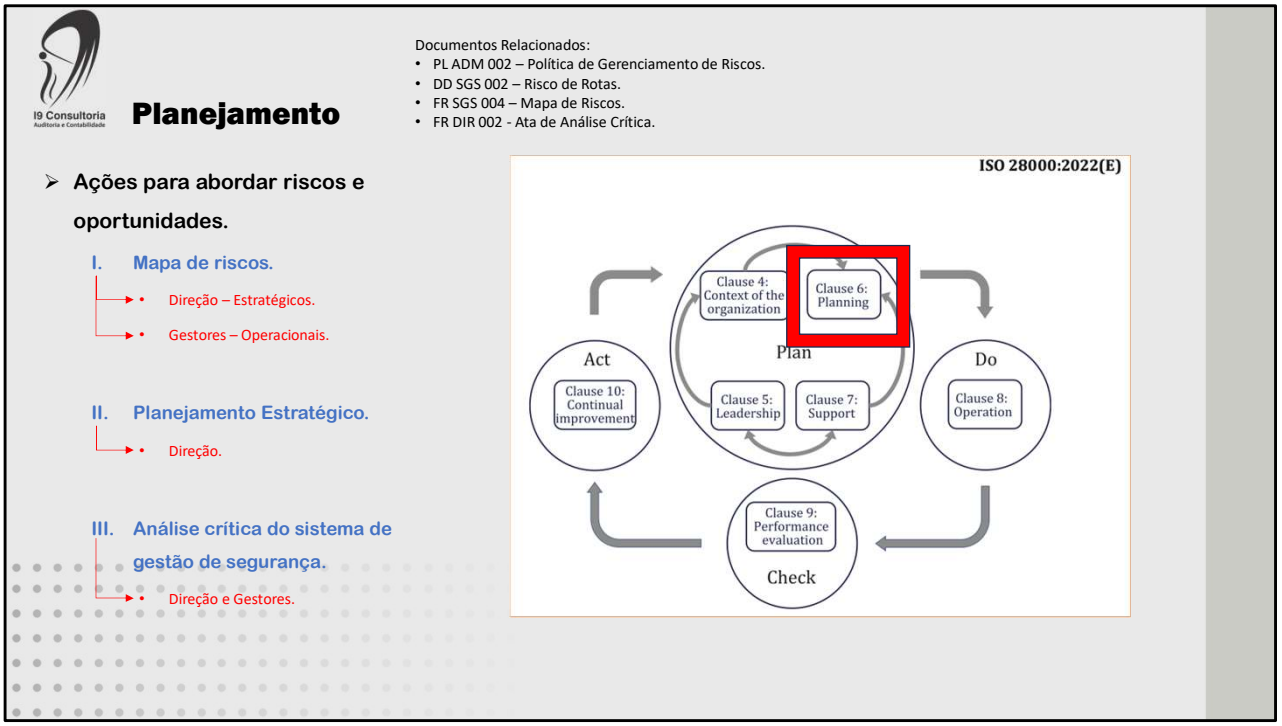
A organização deve:

a) implementar e manter um processo para identificar, ter acesso e avaliar os requisitos legais, regulamentares e outros aplicáveis relacionados à sua segurança;

b) assegurar que estes requisitos legais, regulamentares e outros aplicáveis sejam tidos em conta na implementação e manutenção do seu sistema de gestão de segurança;

c) documentar essas informações e mantê-las atualizadas;

d) comunicar essas informações às partes interessadas relevantes, conforme apropriado.



Ações para abordar riscos e oportunidades:
Ao planejar o sistema de gestão de segurança, a organização deve considerar e determinar os riscos e oportunidades que precisam ser abordados para:
— dar garantias de que o sistema de gestão da segurança pode alcançar o(s) resultado(s) pretendido(s);
— prevenir ou reduzir efeitos indesejáveis;
— alcançar a melhoria contínua.

A organização deve planejar:
a) ações para enfrentar esses riscos e oportunidades;

b) como fazer:
— integrar e implementar as ações nos processos do seu sistema de gestão da segurança;
— avaliar a eficácia destas ações.

A determinação dos riscos relacionados com a segurança e a identificação e exploração de oportunidades requerem uma avaliação proativa dos riscos que deverá incluir a consideração, mas não se limitar a:

a) falhas físicas ou funcionais e atos dolosos ou criminosos;
b) fatores ambientais, humanos e culturais e outros contextos internos ou externos, incluindo fatores fora do controle da organização que afetam a segurança da organização;
c) projeto, instalação, manutenção e substituição de equipamentos de segurança;
a gestão da informação, dos dados, do conhecimento e da comunicação da organização;
e) informações relacionadas a ameaças e vulnerabilidades à segurança;
f) as interdependências entre fornecedores.

A avaliação do risco relacionado com a segurança identificado deve fornecer informações (mas não se limitar a):
a) a gestão geral de riscos da organização;
b) tratamento de risco;
c) objetivos de gestão de segurança;
d) processos de gestão de segurança;
e) a concepção, especificação e implementação do sistema de gestão de segurança;
f) a identificação de recursos adequados, incluindo pessoal;
g) a identificação das necessidades de formação e do nível de competência exigido.

Objetivos de segurança e planejamento para alcançá-los.
A organização deve estabelecer objetivos de segurança nas funções e níveis relevantes.

Os objetivos de segurança devem:
a) ser consistente com a política de segurança;
b) ser mensurável (se praticável);
c) levar em consideração os requisitos aplicáveis;
d) ser monitorado; e) ser comunicado;
e) ser atualizado conforme apropriado;
f) estar disponível como informação documentada.

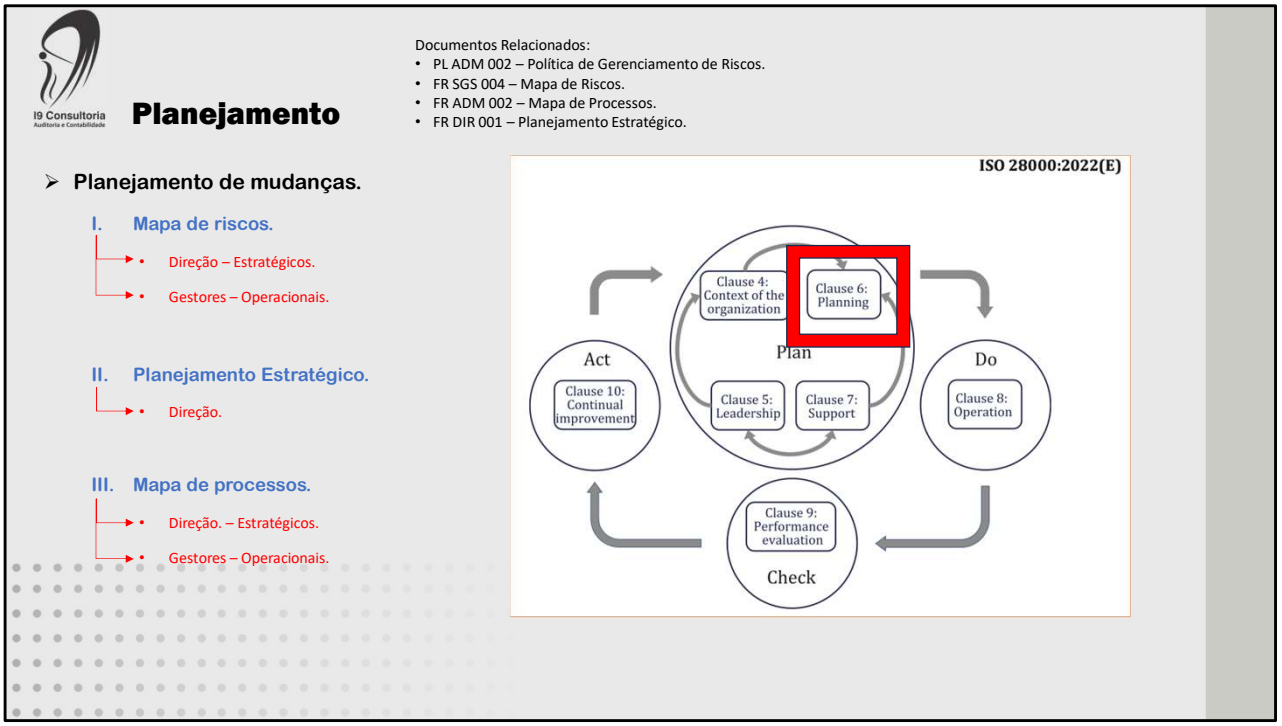
Ao planear como atingir os seus objetivos de segurança, a organização deve determinar:
— o que será feito;
— quais recursos serão necessários;
— quem será o responsável;
— quando será concluído;

— como os resultados serão avaliados.

Ao estabelecer e rever os seus objetivos de segurança, uma organização deve ter em conta:

a) opções tecnológicas, humanas, administrativas e outras;
b) opiniões e impactos nas partes interessadas apropriadas.

Os objetivos de segurança devem ser consistentes com o compromisso da organização de manter melhoria.

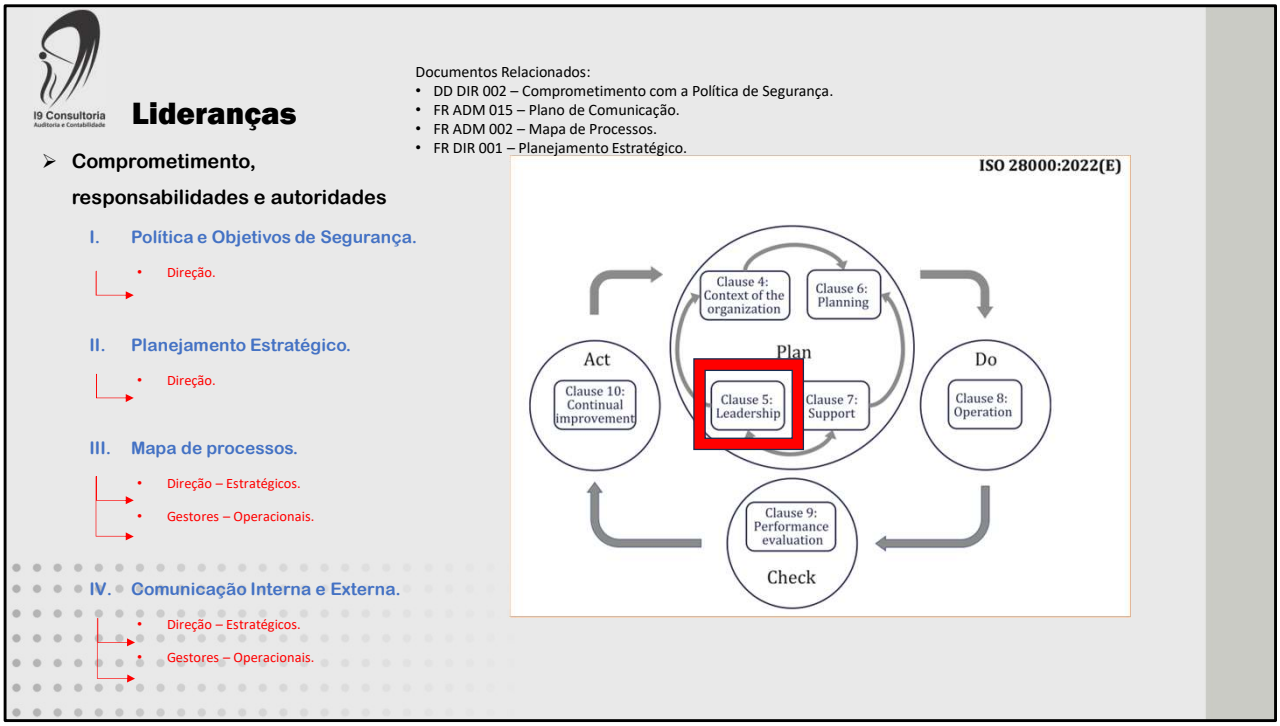


Planejamento de mudanças.

Quando a organização determinar a necessidade de alterações no sistema de gestão de segurança, as alterações devem ser realizadas de forma planeada.

A organização deve considerar:

a) a finalidade das alterações e suas potenciais consequências;
b) a integridade do sistema de gestão de segurança;
c) a disponibilidade de recursos;
d) a atribuição ou realocação de responsabilidades e autoridades.



Liderança e comprometimento

A alta direção deve demonstrar liderança e comprometimento com relação ao sistema de gestão de segurança:

— garantir que a política de segurança e os objetivos de segurança sejam estabelecidos e sejam compatíveis com a direção estratégica da organização;

— garantir que os requisitos e expectativas das partes interessadas da organização sejam identificados e monitorados, e que sejam tomadas medidas apropriadas e oportunas para gerenciar essas expectativas, a fim de garantir a integração dos requisitos do sistema de gestão de segurança nos processos de negócios da organização;

— garantir a integração dos requisitos do sistema de gestão de segurança nos processos de negócios da organização;

— garantir que os recursos necessários para o sistema de gestão da segurança estejam disponíveis;

— comunicar a importância de uma gestão de segurança eficaz e da conformidade com os requisitos do sistema de gestão de segurança;

— assegurar que o sistema de gestão da segurança atinge o(s) resultado(s) pretendido(s);

— assegurar a viabilidade dos objectivos, metas e programas de gestão da

segurança;
— garantir que quaisquer programas de segurança gerados por outras partes da organização complementem o sistema de gestão de segurança;
— orientar e apoiar pessoas para contribuir para a eficácia do sistema de gestão da segurança;
— promover a melhoria contínua do sistema de gestão de segurança da organização;
— apoiar outras funções relevantes para demonstrar a sua liderança no que se refere às suas áreas de responsabilidade.

Política de Segurança

A alta administração deve estabelecer uma política de segurança que:

a) é apropriado ao propósito da organização;
b) fornece uma estrutura para definir objetivos de segurança;
c) inclui o compromisso de atender aos requisitos aplicáveis;
d) inclui um compromisso com a melhoria contínua do sistema de gestão de segurança;
e) considera o impacto adverso que a política de segurança, objectivos, metas, programas, etc. podem ter sobre outros aspectos da organização.

A política de segurança deve:
— ser consistente com outras políticas organizacionais;
— ser consistente com a avaliação geral dos riscos de segurança da organização;
— prever a sua revisão em caso de aquisição ou fusão com outras organizações, ou de outras alterações no âmbito empresarial da organização que possam afetar a

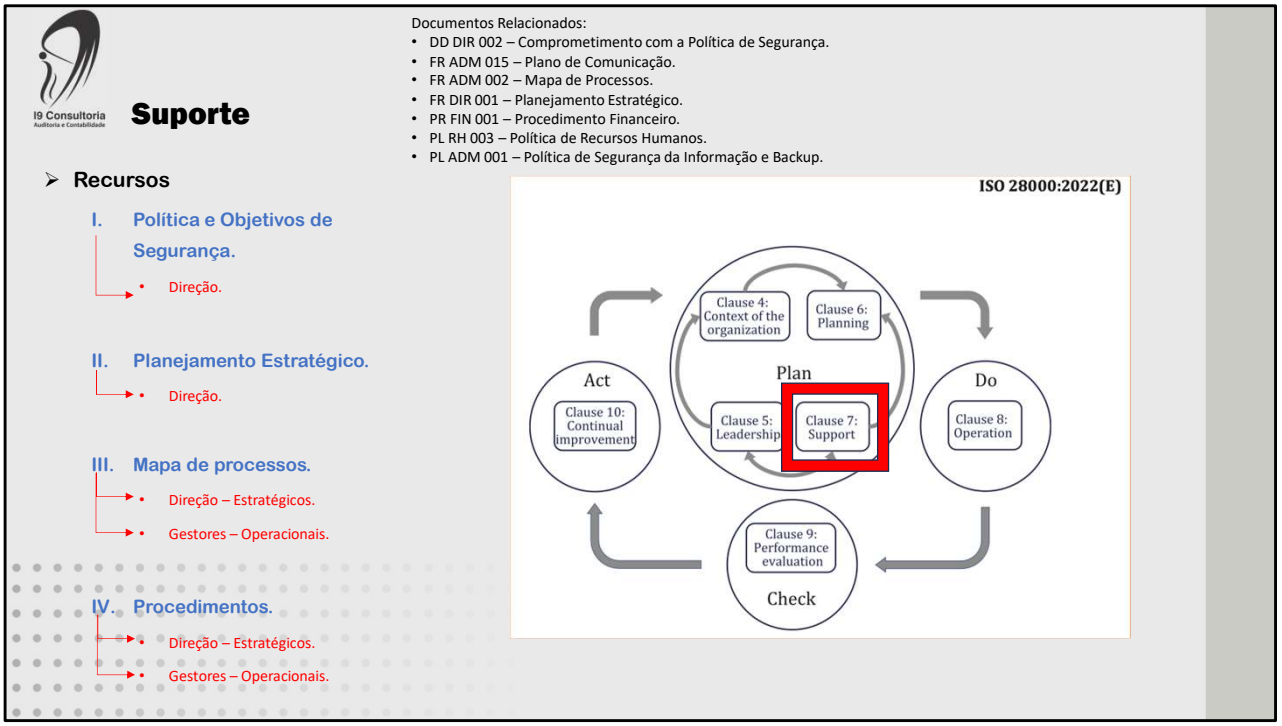
continuidade ou a relevância do sistema de gestão da segurança;
— descrever e atribuir responsabilização primária e responsabilidade pelos resultados;
— estar disponível como informação documentada;
— ser comunicado dentro da organização;
— estar à disposição das partes interessadas, conforme apropriado.

Resopnsabilidades e Autoridades

A gestão de topo deve garantir que as responsabilidades e autoridades para as funções relevantes sejam atribuídas e comunicadas dentro da organização.

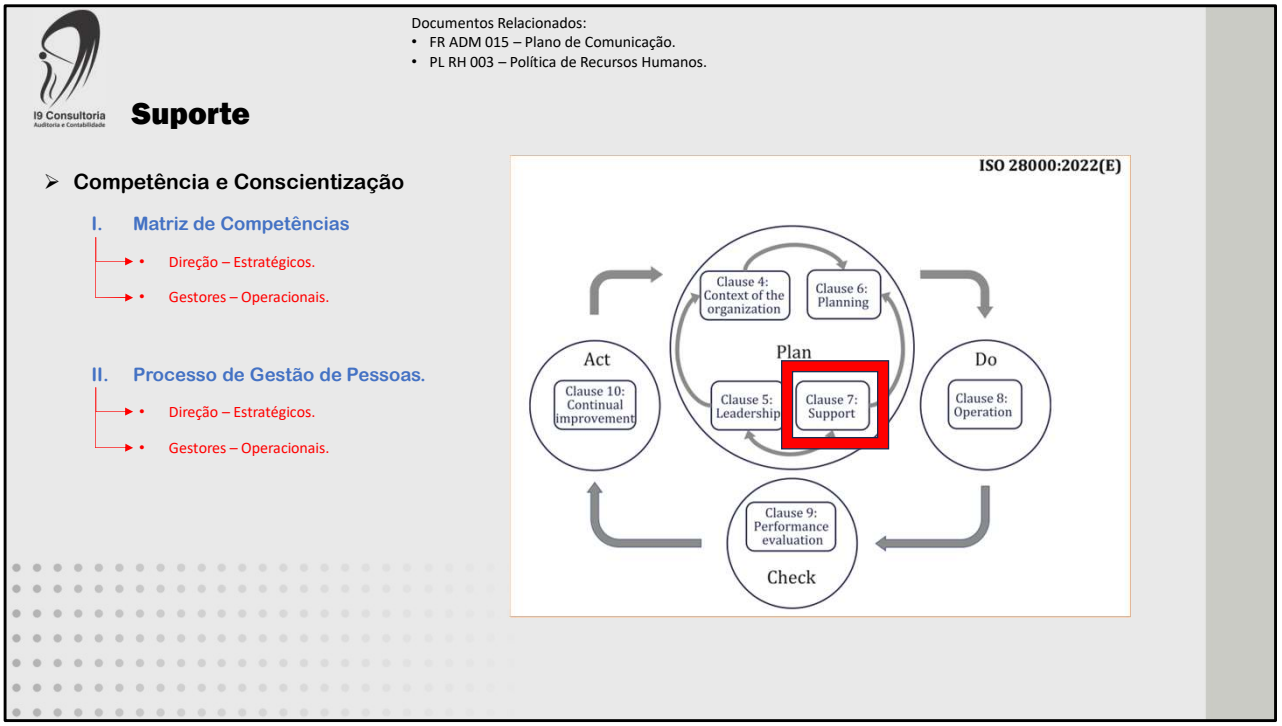
A alta direção deve atribuir a responsabilidade e autoridade para:

a) garantir que o sistema de gestão de segurança esteja em conformidade com os requisitos deste documento;
b) reportar o desempenho do sistema de gestão de segurança à gestão de topo.



Recursos

A organização deve determinar e fornecer os recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão de segurança.



Competências

A organização deve:

— determinar a competência necessária da(s) pessoa(s) que realizam trabalhos sob seu controle que afetam seu desempenho em segurança;

— garantir que essas pessoas sejam competentes com base em educação, formação ou experiência adequadas e possuam credenciação de segurança adequada;

— quando aplicável, tomar medidas para adquirir as competências necessárias e avaliar a eficácia das ações tomadas; Informações documentadas apropriadas deverão estar disponíveis como prova de competência.

NOTA As ações aplicáveis podem incluir, por exemplo: a oferta de formação, a orientação ou a transferência de pessoas atualmente empregadas; ou a contratação ou contratação de pessoas competentes.

Conscientização

As pessoas que realizam trabalho sob o controle da organização devem estar cientes de: — a política de segurança; — a sua contribuição para a eficácia do sistema de gestão da segurança, incluindo os benefícios de um melhor

desempenho da segurança; — as implicações da não conformidade com os requisitos do sistema de gestão da segurança; — as suas funções e responsabilidades no cumprimento da política e dos procedimentos de gestão da segurança e dos requisitos do sistema de gestão da segurança, incluindo os requisitos de preparação e resposta a emergências.

I9 Consultoria
Auditoria e Contabilidade

Suporte

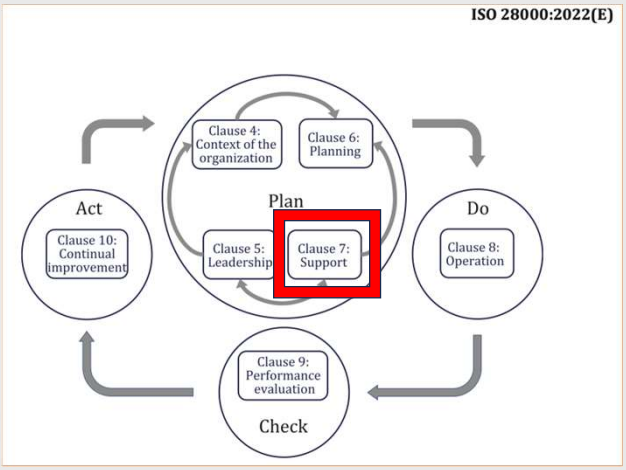
Documentos Relacionados:
- FR ADM 015 – Plano de Comunicação.
- FR ADM 002 – Mapa de Processos.
- FR DIR 001 – Planejamento Estratégico.

➢ **Comunicação**

I. Mapa de riscos.
- Direção – Estratégicos.
- Gestores – Operacionais.

II. Planejamento Estratégico.
- Direção.

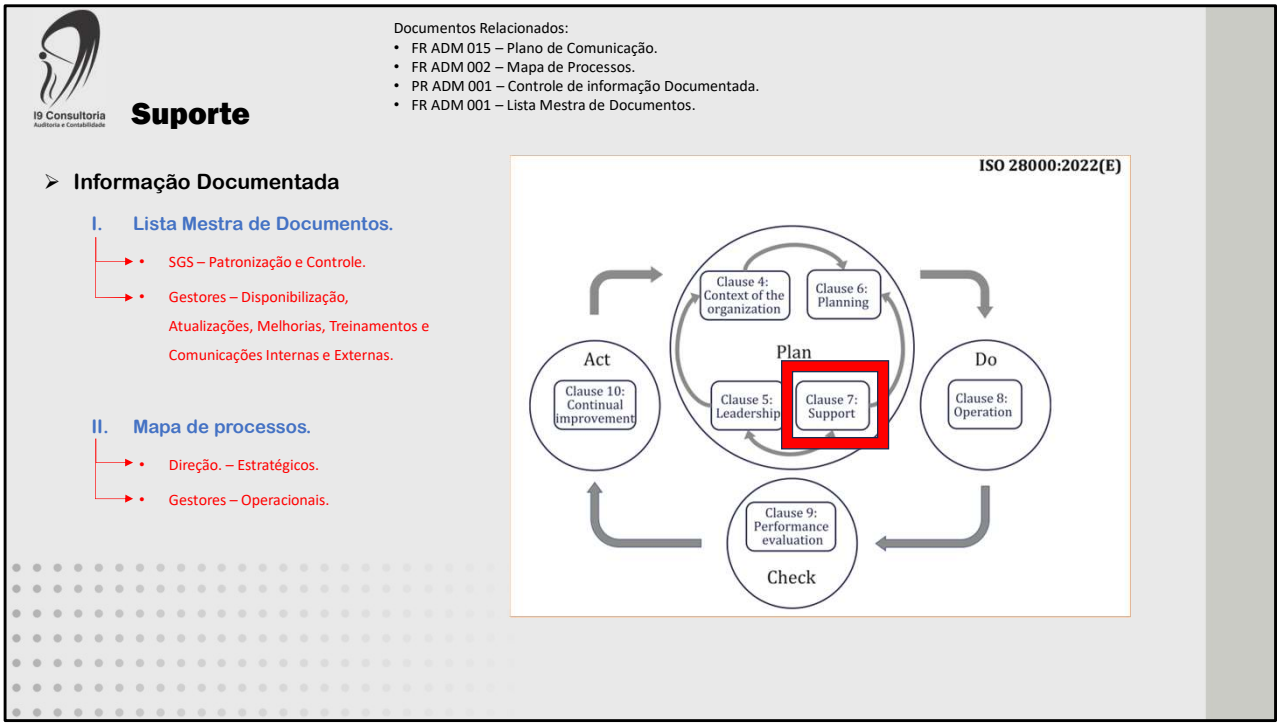
III. Mapa de processos.
- Direção. – Estratégicos.
- Gestores – Operacionais.



Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão da segurança, incluindo:

— sobre o que irá comunicar;
— quando comunicar;
— com quem comunicar;
— como comunicar;
— a sensibilidade da informação antes da divulgação.



Informação Documentada

O sistema de gestão de segurança da organização deve incluir:

a) informações documentadas exigidas por este documento;
b) informações documentadas determinadas pela organização como necessárias para a eficácia do sistema de gestão de segurança.

As informações documentadas devem descrever as responsabilidades e autoridades para alcançar os objetivos e metas de gestão da segurança, incluindo os meios e prazos para atingir esses objetivos e metas.

NOTA A extensão da informação documentada para um sistema de gestão de segurança pode diferir de uma organização para outra devido a:
— a dimensão da organização e o seu tipo de atividades, processos, produtos e serviços;
— a complexidade dos processos e suas interações;
— a competência das pessoas.

A organização deve determinar o valor da informação e estabelecer o nível de integridade exigido e os controles de segurança para impedir o acesso não

autorizado.

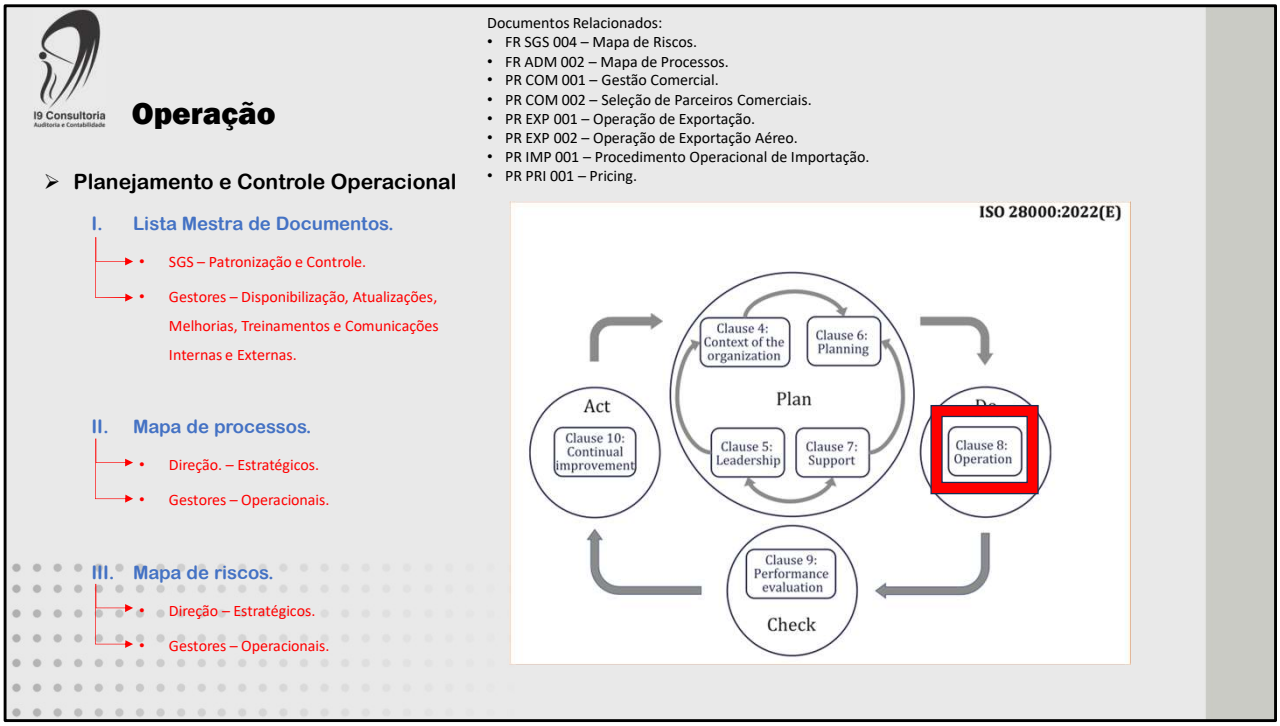
Criação e Atualização
Ao criar e atualizar informações documentadas, a organização deve garantir:
— identificação e descrição (por exemplo, título, data, autor ou número de referência).

Controle de Informação Documentada
As informações documentadas exigidas pelo sistema de gestão de segurança e por este documento devem ser controlado para garantir:

a) está disponível e é adequado para uso, onde e quando for necessário;
b) esteja adequadamente protegido (por exemplo, contra perda de confidencialidade, uso indevido ou perda de integridade);
c) é revisado e revisado periodicamente conforme necessário, e aprovado quanto à adequação por pessoal autorizado;
d) documentos, dados e informações obsoletos sejam prontamente removidos de todos os pontos de emissão e de uso, ou de outra forma protegidos contra uso não intencional;
e) documentos arquivísticos, dados e informações retidos para fins legais ou de preservação de conhecimento ou ambos estejam devidamente identificados.

Para o controle da informação documentada, a organização deve abordar as seguintes atividades, conforme aplicável:
— distribuição, acesso, recuperação e utilização;
— armazenamento e preservação, incluindo preservação da legibilidade;
— controle de alterações (por exemplo, controle de versão);
— retenção e disposição.

As informações documentadas de origem externa determinadas pela organização como necessárias para o planejamento e operação do sistema de gestão de segurança devem ser identificadas, conforme apropriado, e controladas. NOTA O acesso pode implicar uma decisão relativa à permissão para visualizar apenas as informações documentadas, ou a permissão e autoridade para visualizar e alterar as informações documentadas.



Planejamento e controle operacional

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos e implementar as ações determinadas no Planejamento, através de:

— estabelecer critérios para os processos;

— implementar o controle dos processos de acordo com os critérios.

As informações documentadas devem estar disponíveis na medida necessária para garantir que os processos foram executados conforme planejado.

Planejamento e controle operacional

A organização deve identificar os processos e atividades que são necessários para alcançar:

a) cumprimento de sua política de segurança;

b) cumprimento dos requisitos de segurança legais, estatutários e regulamentares;

Avaliação e tratamento de riscos

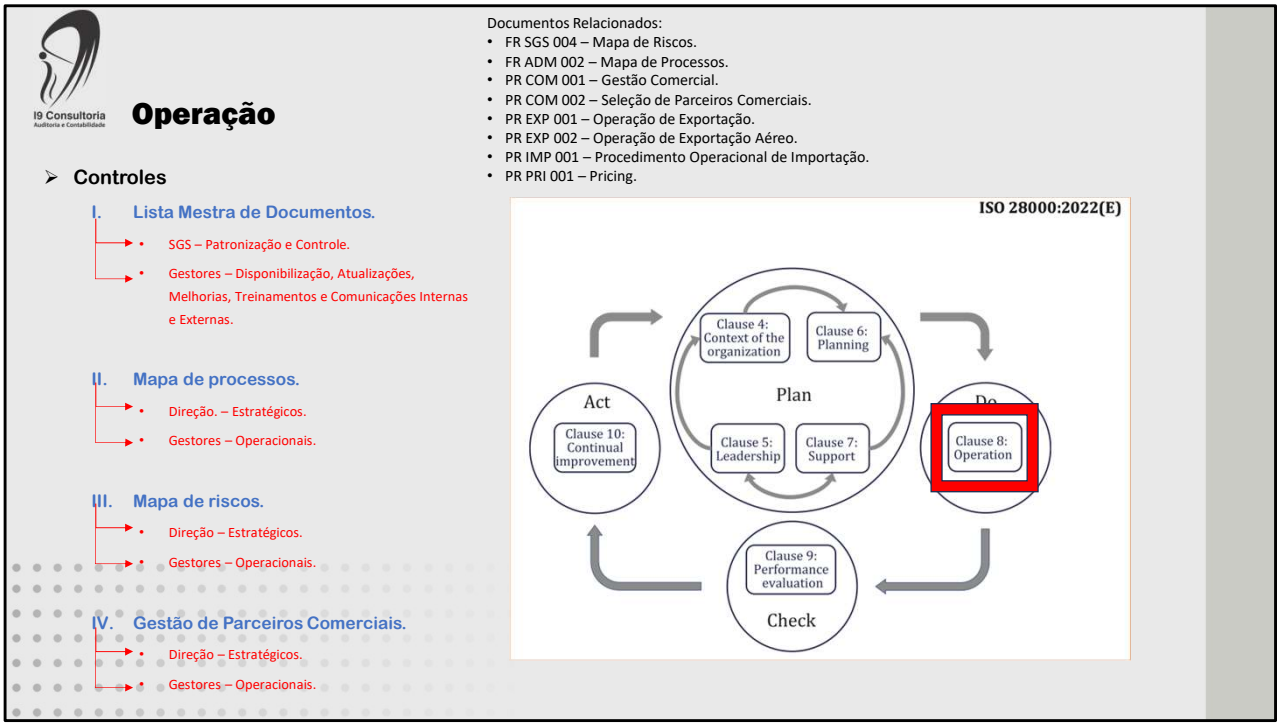
A organização deve implementar e manter um processo de avaliação e tratamento de riscos.

NOTA O processo de avaliação e tratamento de riscos é abordado na ISO 31000.

A organização deve:

a) identificar seus riscos relacionados à segurança, priorizando-os em relação aos recursos necessários à sua gestão de segurança;
b) analisar e avaliar os riscos identificados;
c) determinar quais riscos requerem tratamento;
d) selecionar e implementar opções para lidar com esses riscos;
e) elaborar e implementar planos de tratamento de riscos.

NOTA Os riscos nesta subcláusula referem-se à segurança da organização e de suas partes interessadas. Os riscos e oportunidades relacionados com a eficácia do sistema de gestão são abordados em 6.1.



Controles

Os processos listados devem incluir controles para gestão de:

a) recursos humanos, bem como;
b) o projeto,
c) instalação,
d) operação,
e) reforma e modificação de itens de equipamentos;
f) instrumentação e tecnologia da informação relacionados à segurança, conforme apropriado.

Quando os acordos existentes forem revistos ou forem introduzidos novos acordos que possam ter impacto na gestão da segurança, a organização deve considerar os riscos relacionados com a segurança associados antes da sua implementação.

Os acordos novos ou revisados a serem considerados incluirão:

a) estrutura organizacional, funções ou responsabilidades revisadas;
b) formação, sensibilização e gestão de recursos humanos;
c) política, objectivos, metas ou programas revistos de gestão da segurança;

d) processos e procedimentos revisados;
e) a introdução de novas infraestruturas, equipamentos ou tecnologias de segurança, que podem incluir hardware e/ou software;
f) a introdução de novos contratados, fornecedores ou pessoal, conforme o caso;
g) os requisitos para garantia de segurança de fornecedores externos. A organização deve controlar as alterações planeadas e rever as consequências das alterações não intencionais, tomando medidas para mitigar quaisquer efeitos adversos, conforme necessário. A organização deve garantir que os processos, produtos ou serviços fornecidos externamente que sejam relevantes para o sistema de gestão da segurança sejam controlados.

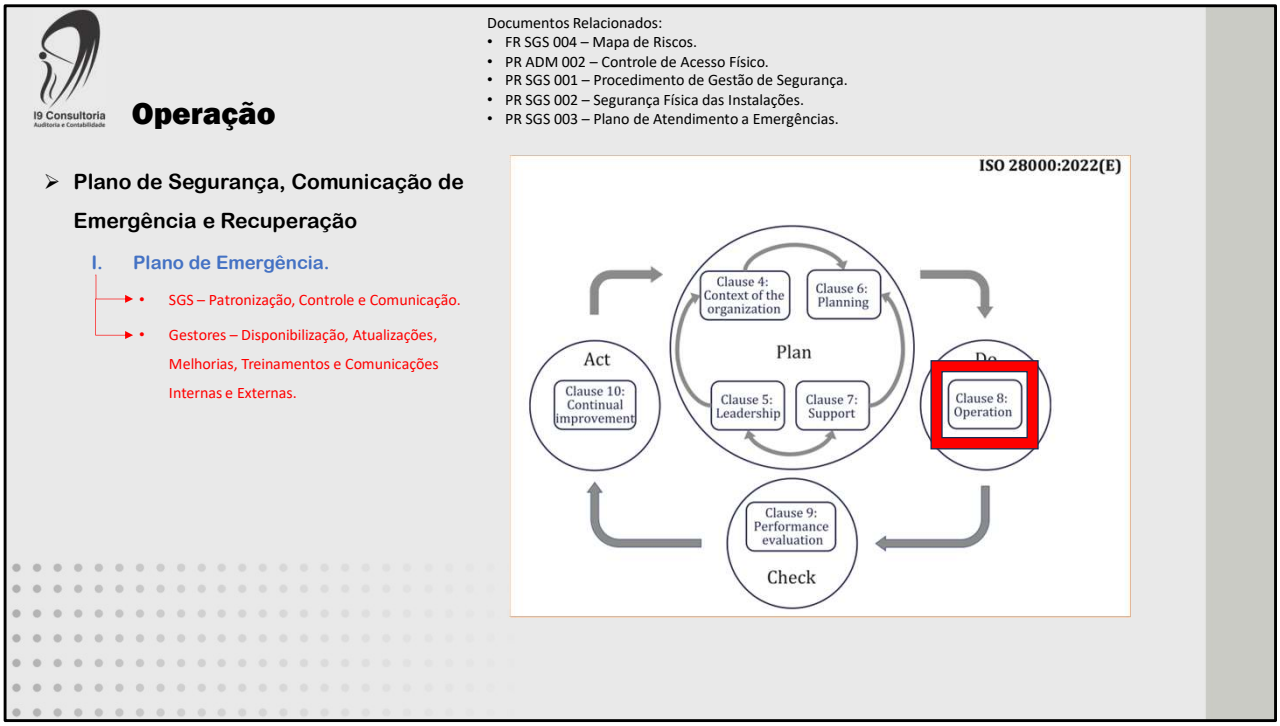
Estratégias, Procedimentos, Processos e Tratamentos de Segurança

A organização deve implementar e manter processos sistemáticos para análise de vulnerabilidades e ameaças relacionadas à segurança. Com base nesta análise de vulnerabilidades e ameaças e consequente avaliação de riscos, a organização deve identificar e selecionar uma estratégia de segurança que compreenda um ou mais procedimentos, processos e tratamentos.
A identificação deve basear-se na medida em que estratégias, procedimentos, processos e tratamentos:
a) manter a segurança da organização;
b) reduzir a probabilidade de vulnerabilidade de segurança;
c) reduzir a probabilidade de uma ameaça se concretizar;
d) encurtar o período de quaisquer deficiências no tratamento de segurança e limitar o seu impacto;
e) prever a disponibilidade de recursos adequados.

A seleção deve basear-se na medida em que as estratégias, processos e tratamentos:
— atender aos requisitos para proteger a segurança da organização;
— considerar a quantidade e o tipo de risco que a organização pode ou não assumir;
— considerar os custos e benefícios associados.

A organização deve determinar os requisitos de recursos para implementar os procedimentos, processos e tratamentos de segurança selecionados.

A organização deve implementar e manter tratamentos de segurança selecionados.



Estrutura de Resposta

A organização deve implementar e manter uma estrutura, identificando uma pessoa designada ou uma ou mais equipas responsáveis por responder a vulnerabilidades e ameaças relacionadas com a segurança. As funções e responsabilidades da pessoa designada ou de cada equipe e o relacionamento entre a pessoa ou equipes devem ser claramente identificados, comunicados e documentados. Coletivamente, as equipes deverão ser competentes para: a) avaliar a natureza e a extensão de uma ameaça à segurança e o seu impacto potencial;

Comunicação de Emergência

A organização deve documentar e manter procedimentos para:

a) comunicar-se interna e externamente com as partes interessadas relevantes, incluindo o que, quando, com quem e como comunicar; NOTA A organização pode documentar e manter procedimentos sobre como e sob quais circunstâncias a organização se comunica com os funcionários e seus contatos de emergência.

b) receber, documentar e responder às comunicações das partes interessadas, incluindo qualquer sistema nacional ou regional de aconselhamento de risco

ou equivalente;
c) garantir a disponibilidade dos meios de comunicação durante uma violação, vulnerabilidade ou ameaça de segurança;
d) facilitar a comunicação estruturada com as equipes de resposta a ameaças e/ou violações de segurança;
e) fornecer detalhes da resposta da mídia da organização após uma violação de segurança, incluindo uma estratégia de comunicação;
f) registrar os detalhes da violação de segurança, as ações tomadas e as decisões tomadas.

Quando aplicável, o seguinte também deve ser considerado e implementado:
— alertar as partes interessadas potencialmente afetadas por uma violação de segurança real ou iminente;
— assegurar a coordenação e a comunicação adequadas entre as múltiplas organizações respondentes.

Os procedimentos de alerta e comunicação devem ser exercidos como parte do programa de testes e treinamento da organização.

Conteúdo do Plano de Segurança
A organização deve documentar e manter planos de segurança. Esses planos devem fornecer orientação e informações para ajudar as equipes a responder a uma vulnerabilidade, ameaça e/ou violação de segurança e para ajudar a organização na resposta e na restauração de sua segurança. Coletivamente, os planos de segurança devem conter:
a) detalhes das ações que as equipes realizarão para:
    1) continuar ou restaurar o status de segurança acordado;
    2) monitorar o impacto das ameaças, vulnerabilidades ou violações de segurança reais ou iminentes e a resposta da organização a elas;

b) referência ao(s) limiar(es) e processo predefinidos para ativação da resposta;
c) procedimentos para restaurar a segurança da organização;
d) detalhes para gerenciar as consequências imediatas de uma vulnerabilidade e ameaça de segurança ou violação de segurança real ou iminente, dando a devida atenção a:
    1) o bem-estar dos indivíduos;
    2) o valor dos bens, informações e pessoal potencialmente comprometidos;
    3) a prevenção de (adicionais) perdas ou indisponibilidade de atividades essenciais.

Cada plano deve incluir:

— a sua finalidade, âmbito e objetivos;
— as funções e responsabilidades da equipe que implementará o plano;
— as ações para implementar as soluções;
— as informações necessárias para ativar (incluindo critérios de ativação), operar, coordenar e comunicar as ações da equipe;
— interdependências internas e externas;
— as suas necessidades de recursos;
— os seus requisitos de apresentação de relatórios;
— um processo para desistir.

Cada plano deve ser utilizável e estar disponível no momento e local em que for necessário. 8.6.5 Recuperação A organização deve ter processos documentados para restaurar a segurança da organização contra quaisquer medidas temporárias adotadas antes, durante e depois de uma violação de segurança.

Avaliação de Performance

Documentos Relacionados:
- FR ADM 015 – Plano de Comunicação.
- FR ADM 002 – Mapa de Processos.
- FR DIR 001 – Planejamento Estratégico.
- FR SGS 004 – Mapa de Riscos.
- FR DIR 002 - Ata de Análise Crítica.

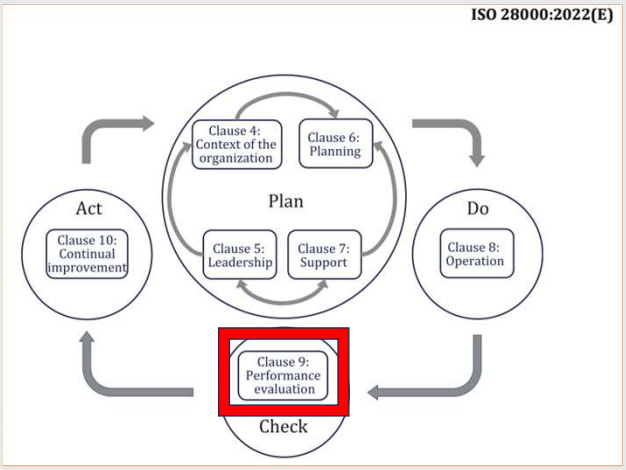
➢ **Monitoramento, Medição, Análise e Avaliação**

I. Mapa de processos.
- Direção. – Estratégicos.
- Gestores – Operacionais.
- SGS – Padronização e Controle.

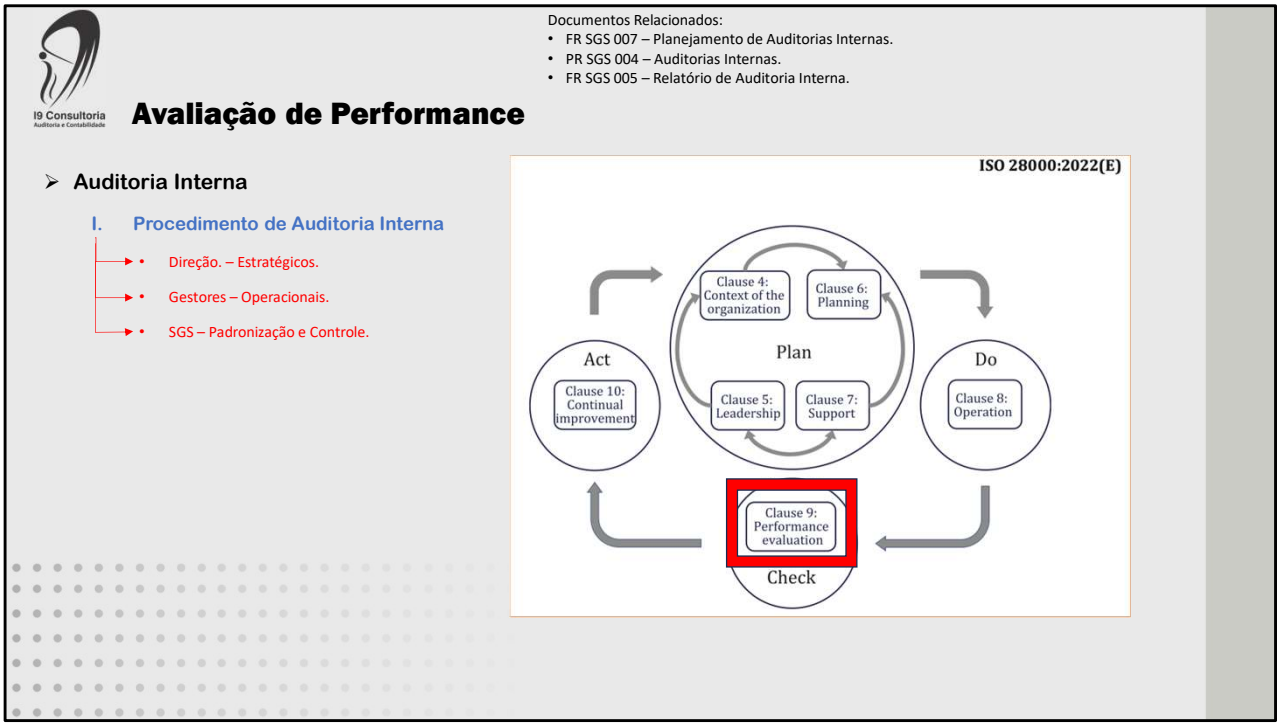
II. Mapa de riscos.
- Direção – Estratégicos.
- Gestores – Operacionais.

III. Planejamento Estratégico.
- Direção.

IV. Análise crítica do sistema de gestão de segurança.
- Direção e Gestores.



A organização deve determinar:
— o que precisa ser monitorado e medido;
— os métodos de monitoramento, medição, análise e avaliação, conforme aplicável, para garantir resultados válidos;
— quando o monitoramento e a medição serão realizados;
— quando os resultados do monitoramento e da medição serão analisados e avaliados.



A organização deve realizar auditorias internas em intervalos planejados para fornecer informações sobre se o sistema de gestão de segurança:

a) está em conformidade com:
    1) os próprios requisitos da organização para o seu sistema de gestão de segurança;
    2) os requisitos deste documento;

b) seja efetivamente implementado e mantido. 9.2.2 Programa de auditoria interna A organização deve planejar, estabelecer, implementar e manter programa(s) de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Ao estabelecer o(s) programa(s) de auditoria interna, a organização deve considerar a importância dos processos em questão e os resultados de auditorias anteriores.

A organização deve:

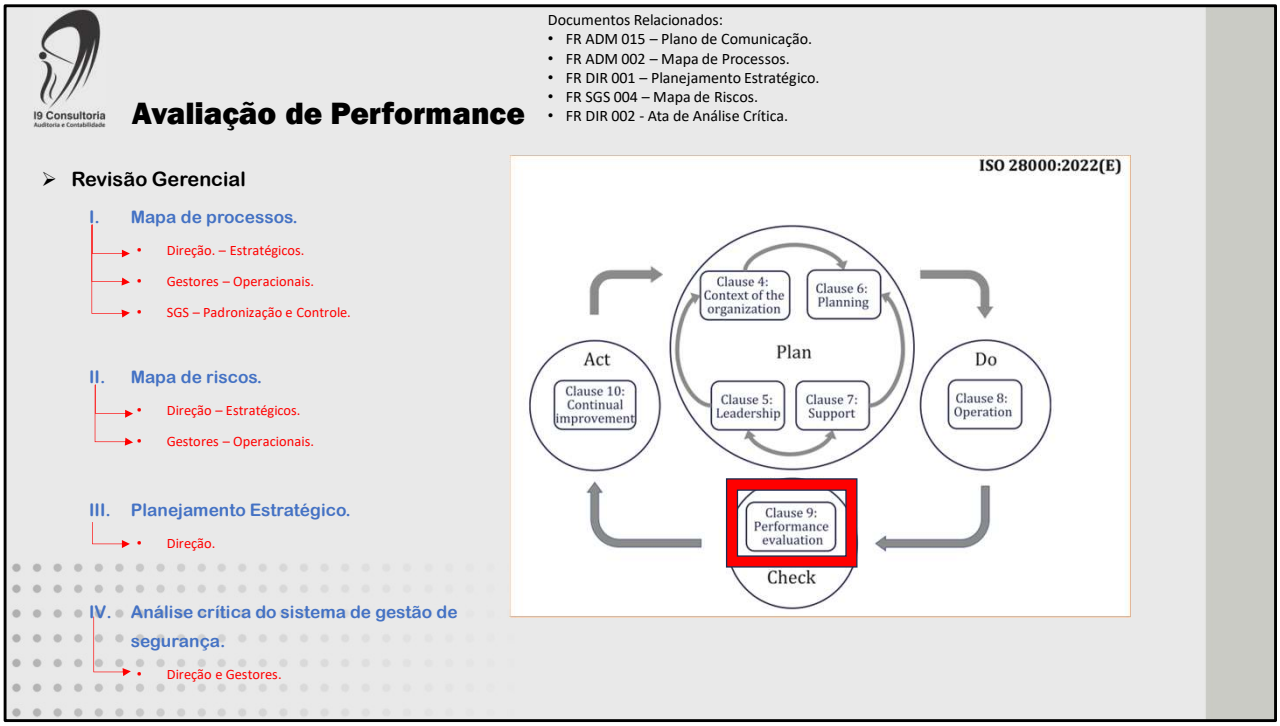
a) definir os objetivos, critérios e escopo da auditoria para cada auditoria;
b) selecionar auditores e realizar auditorias para garantir a objetividade e a imparcialidade do processo de auditoria;

c) garantir que os resultados das auditorias sejam reportados aos gestores relevantes.
d) verificar se o equipamento e o pessoal de segurança estão adequadamente mobilizados;
e) garantir que quaisquer ações corretivas necessárias sejam tomadas sem demora injustificada para eliminar as não conformidades detectadas e suas causas;
f) garantir que as ações de auditoria de acompanhamento incluam a verificação das ações tomadas e a comunicação dos resultados da verificação.

As informações documentadas devem estar disponíveis como prova da implementação do(s) programa(s) de auditoria e dos resultados da auditoria.

O programa de auditoria, incluindo qualquer cronograma, deve basear-se nos resultados das avaliações de risco das atividades da organização e nos resultados de auditorias anteriores.

Os procedimentos de auditoria devem abranger o âmbito, a frequência, as metodologias e as competências, bem como as responsabilidades e os requisitos para a realização de auditorias e a comunicação de resultados.



Revisão Geral

A gestão de topo deve rever o sistema de gestão de segurança da organização, em intervalos planeados, para garantir a sua adequação, adequação e eficácia contínuas.

A organização deve considerar os resultados da análise e avaliação, e os resultados da revisão pela gestão, para determinar se existem necessidades ou oportunidades relacionadas com o negócio ou com o sistema de gestão de segurança que devem ser abordadas como parte da melhoria contínua. NOTA A organização pode utilizar os processos do sistema de gestão de segurança, tais como liderança, planejamento e avaliação de desempenho, para alcançar melhorias.

A revisão pela gestão deve incluir:

a) o status das ações de revisões gerenciais anteriores;

b) alterações em questões externas e internas relevantes para o sistema de gestão de segurança;

c) mudanças nas necessidades e expectativas das partes interessadas que sejam relevantes para o sistema de gestão de segurança;

d) informações sobre o desempenho da segurança, incluindo tendências em:

1) não conformidades e ações corretivas;

2) resultados de monitoramento e medição;

3) resultados da auditoria;

e) oportunidades de melhoria contínua;

f) resultados de auditorias e avaliações do cumprimento dos requisitos legais e outros requisitos que a organização subscreva;

g) comunicações de partes interessadas externas, incluindo reclamações;

h) o desempenho de segurança da organização;

i) até que ponto os objetivos e metas foram alcançados;

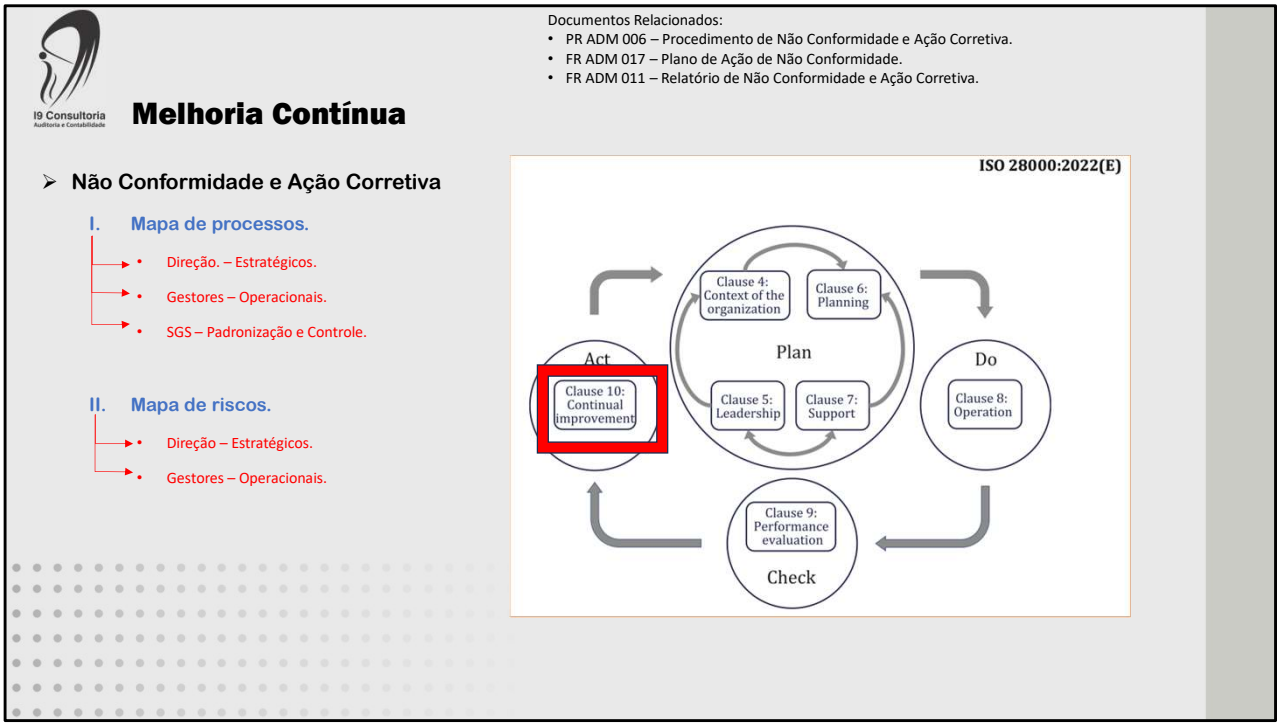
j) situação das ações corretivas;

k) ações de acompanhamento de revisões gerenciais anteriores;

l) mudanças nas circunstâncias, incluindo desenvolvimentos em requisitos legais, regulatórios e outros (ver 4.2.2) relacionados a aspectos de segurança;

m) recomendações de melhoria.

Os resultados da revisão pela gestão devem incluir decisões relacionadas com oportunidades de melhoria contínua e qualquer necessidade de alterações no sistema de gestão da segurança. Informações documentadas devem estar disponíveis como prova dos resultados das análises pela gestão.



Não Conformidade a Ação Corretiva

Quando ocorrer uma não conformidade, a organização deve:

a) reagir à não conformidade e, conforme aplicável:
   1) tomar medidas para controlá-lo e corrigi-lo;
   2) lidar com as consequências;

b) avaliar a necessidade de ação para eliminar a(s) causa(s) da não conformidade, para que ela não se repita ou ocorra em outro lugar, por meio de:
   1) revisão da não conformidade;
   2) determinação das causas da não conformidade;
   3) determinar se existem ou podem ocorrer não conformidades semelhantes;

c) implementar qualquer ação necessária;
d) analisar a eficácia de quaisquer ações corretivas tomadas;
e) fazer alterações no sistema de gestão de segurança, se necessário.

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas. Informações documentadas devem estar disponíveis como

evidência de:
— a natureza das não conformidades e quaisquer ações subsequentes tomadas;
— os resultados de qualquer ação corretiva;
— a investigação de questões relacionadas com a segurança:
— falhas, incluindo quase acidentes e alarmes falsos;
— incidentes e situações de emergência;
— não conformidades;
— tomar medidas para mitigar quaisquer consequências decorrentes de tais falhas, incidentes ou não conformidades.

Os procedimentos exigirão que todas as ações corretivas propostas sejam revisadas através do processo de avaliação de riscos relacionados à segurança antes da implementação, a menos que a implementação imediata evite exposições iminentes à vida ou à segurança pública. Qualquer ação corretiva tomada para eliminar as causas de não conformidades reais e potenciais deverá ser apropriada à magnitude dos problemas e proporcional aos riscos relacionados ao gerenciamento de segurança que provavelmente serão encontrados.


I9 Consultoria
Auditoria e Treinamentos
Muito obrigado pela sua atenção e um ótimo trabalho para todos nós!!!