Política de **Gestão de Riscos e Controles Internos**

CORSAN

Controle de Alterações

Versão	Data	Descrição
1	19.05.2017	Lançamento da Política de Gestão de Riscos Corporativos
2	02.09.2020	Revisão, adequação ao Código Brasileiro de Governança e ao Regulamento do Novo Mercado da B3, incorporação da Política de Controles Internos

Alçadas de Aprovação

Função	Responsável	Instrumento de Homologação	Data de Aprovação
Pré-aprovação Versão 1	Diretoria Colegiada	Ata 14/2017	13.03.2017
Aprovação Versão 1	Conselho de Administração	Ata 09/2017	19.05.2017
Pré-aprovação Versão 2	Diretoria Colegiada	Ata 46/2020	24.08.2020
Aprovação Versão 2	Conselho de Administração	Ata 14/2020	02.09.2020

Versão 1 elaborada e revisada por:
Departamento de Gestão de Riscos – DEGER/SUCORP

Versão 2 revisada e adequada por:
Departamento de Gestão de Riscos – DEGER/SUCORP

Aprovado por:
Conselho de Administração

1 OBJETIVOS

A Política de Gestão de Riscos e Controles Internos - PGERCI - tem por finalidade, à luz da unificação de conceitos de gestão de riscos e de controles internos (estes como ferramentas de gestão), reduzir os riscos existentes e/ou os que possam se manifestar no futuro, maximizando as oportunidades de negócio e o atingimento dos objetivos estratégicos da Companhia, bem como disseminar a cultura de gestão de riscos e controles internos, para auxiliar na mitigação dos riscos e garantir o cumprimento de leis, regulamentos e normativas internas e externas. Para tanto, é necessário:

a. **conhecer** com profundidade os riscos que afetam a Companhia, considerando a probabilidade de ocorrência e seus possíveis impactos sobre os processos organizacionais;

b. **constituir** diretrizes e competências, assim como consolidar conceitos sobre gestão de riscos e controles internos em todos os níveis da organização;

c. **incentivar** e apoiar as boas práticas de governança corporativa, com enfoque na gestão de riscos e controles internos aplicada a todos os processos da empresa, melhorando a identificação de oportunidades e ameaças, mensurando os resultados com base em dados confiáveis e auxiliando a Administração na tomada de decisão;

d. **promover** maior transparência e confiabilidade das informações e dos resultados, ampliando a credibilidade da Companhia em relação a todas as partes interessadas, contribuindo para sua sustentabilidade; e

e. **instrumentalizar** a Administração na definição do apetite ao risco no processo decisório, na busca do cumprimento dos objetivos organizacionais, e da criação, preservação e crescimento de valor.

2 ABRANGÊNCIA

A PGERCI aplica-se a todos os macroprocessos e operações de negócio da Companhia, devendo ser conhecida e praticada por todos os colaboradores da Corsan (diretores, conselheiros, membros de comitês, empregados, estagiários e aprendizes).

3 REGULAMENTAÇÃO

A presente Política tem como principais referenciais normativos:

- Lei nº 6.404/76 – Lei das Sociedades por Ações;
- Lei Federal nº 13.303/16 – Estatuto Jurídico das Empresas Estatais;
- Decreto Estadual 54.110/18 – Regulamenta a Lei das Estatais no Estado do RS;
- Instrução CVM 586/17 – Instituiu o Código Brasileiro de Governança Corporativa.
- Estatuto Social e Código de Ética e Conduta da Corsan.

4 CONCEITOS

Os conceitos definidos nesta seção objetivam facilitar a compreensão da PGERCI e do Manual de Gestão de Riscos e Controles Internos, parte integrante desta Política:

4.1 **Administração**: Consideram-se administradores da Corsan os membros do Conselho de Administração e da Diretoria Colegiada.

4.2 ***Stakeholders*:** São as partes interessadas, compreendendo todos os entes envolvidos com os negócios e operações da Companhia, com destaque para colaboradores, acionistas, clientes, poder concedente, fornecedores, entes públicos e governamentais, e comunidade em geral.

4.3 **Governança Corporativa:** Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre acionistas, Conselho de Administração, Diretoria, órgãos de fiscalização e controle e demais partes interessadas.

4.4 **Boas práticas:** As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da Companhia**,** sua longevidade e o bem comum.

4.5 **Evento:** Incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

4.6 **Impacto:** Resultado ou efeito de um evento. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos de uma organização.

4.7 **Probabilidade:** Na gestão de riscos, a probabilidade é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos.

4.8 **Incerteza:** é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento e sua compreensão, ao seu conhecimento, à probabilidade de o evento acontecer e às suas consequências.

4.9 **Efeito:** é um desvio em relação ao esperado – positivo e/ou negativo. Os efeitos podem ter diferentes aspectos (tais como metas financeiras, metas de desempenho, de saúde e segurança, ambientais etc.) e podem aplicar-se em diferentes níveis, tais como estratégico, organizacional, de projeto, de produto, de processo e outros.

4.10 Risco: Efeito da incerteza nos objetivos. O risco é, muitas vezes, caracterizado pela referência aos eventos potenciais e às suas consequências, ou uma condição destes. O risco é comumente expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada. Muitos riscos são inerentes ao negócio, e a competência da gestão de riscos e controles reside na seleção de quais riscos a empresa deve tratar prioritariamente;

4.11 Controles Internos: Procedimentos desenvolvidos para garantir, com razoável certeza, que sejam atingidos os objetivos da organização, modificando os riscos do negócio, seja reduzindo a probabilidade de sua ocorrência, seja minimizando seus impactos negativos. Os controles internos incluem qualquer processo, definição e aplicação de política, dispositivos, práticas ou outras ações direcionadas à modificação dos riscos. Os controles internos compreendem todos os métodos e medidas adotadas pela empresa para salvaguardar seus ativos, verificar a exatidão e fidelidade dos dados e informações contábeis, desenvolver a eficiência nas operações e encorajar a adesão de todos os níveis da organização às políticas traçadas pela Administração. Entretanto, os controles nem sempre conseguem exercer o efeito pretendido ou presumido de modificação dos riscos, sendo necessários monitoramento e aperfeiçoamento constantes.

4.12 Apetite ao risco: Quantidade e tipos de riscos que uma organização está preparada para buscar, manter ou assumir. É o processo em que se consideram os efeitos conjuntos resultantes de diferentes riscos ou dos efeitos do mesmo risco em vários sistemas, várias áreas de negócio ou diferentes processos da organização.

4.13 **Cultura de Gestão de Riscos e Controles Internos:** a gestão de riscos e controles internos deve promover alterações na forma de pensar, agir e aplicar políticas em processos, as quais devem estar fundamentadas em boas estratégias e no fortalecimento do ambiente de controle da empresa. Essa cultura, se adotada uniforme e capilarmente, trará benefícios na melhoria da gestão da Companhia e na geração de valor e resultado para os investidores e demais partes interessadas, considerando a disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis.

4.14 ***KPI – Key Performance Indicators*:** Indicadores-chave de desempenho, têm por finalidade medir a etapa de um processo ou sistema, com acompanhamento periódico dos resultados apresentados, auxiliando na avaliação e identificação de possíveis problemas ou dificuldades, considerando que diversas são as metas instituídas pela organização às atividades exercidas por seus colaboradores. Um KPI pode ser um dado ou uma razão, mas é mais comum ser uma razão (por exemplo, ocorrências de reclamações por atendimento).

4.15 ***KRI – Key Risk Indicators*:** Indicadores-chave de risco, são métricas utilizadas pela organização para determinar qual o seu potencial de exposição a um determinado risco, monitorando os níveis de risco de áreas específicas da empresa ou da organização como um todo, fornecendo informações significativas para o atingimento de metas estratégicas e sinalizando a necessidade de ações a serem tomadas com maior tempestividade.

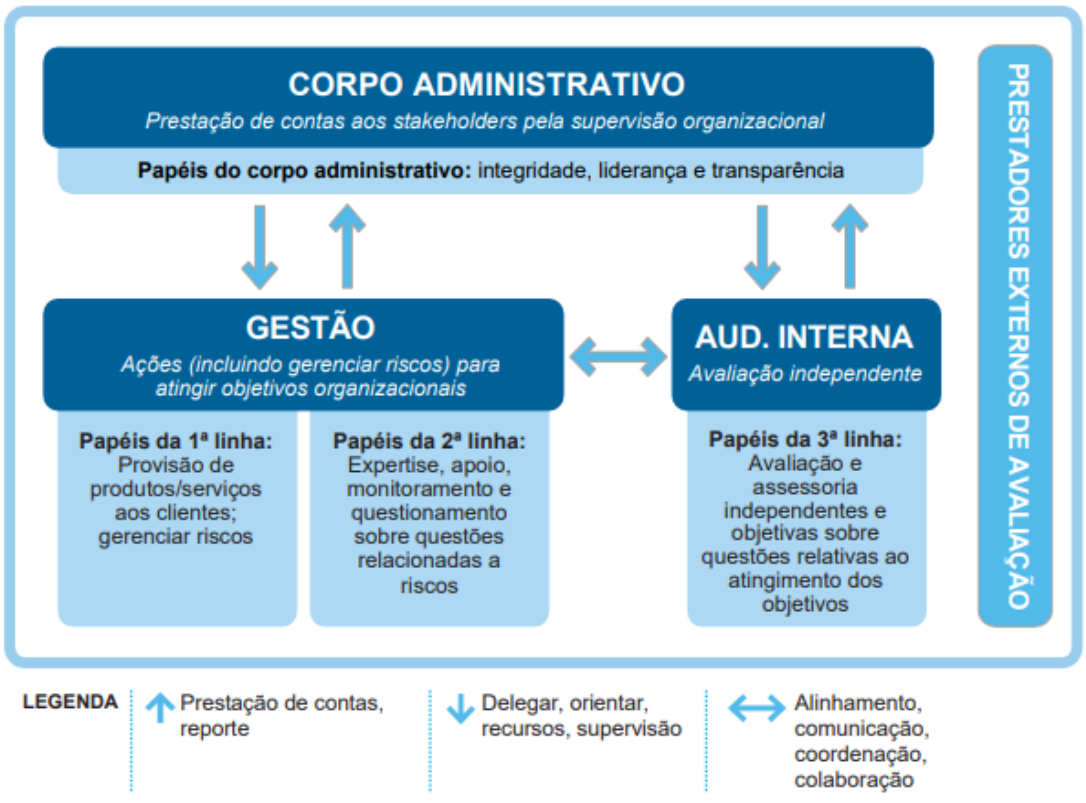
4.16 **Maturidade do modelo de gestão de riscos:** espelha a compreensão do estágio em que se encontram os processos de gestão e governança de riscos da organização. Para a avaliação da maturidade, devem ser consideradas as ações adotadas para alcance de metas e objetivos da gestão de riscos, o esforço em tempo e investimento, a medição da eficácia e eficiência das práticas adotadas, o envolvimento dos profissionais, o entendimento do processo de gestão de riscos como parte da cultura, as estruturas organizacionais envolvidas com gestão de riscos, a consideração de como os riscos são integrados no processo decisório em todos os níveis e a governança do processo no seu todo;

4.17 **Modelo das Três Linhas:** O modelo das três linhas do IIA (*The Institute of Internal Auditors* – Instituto dos Auditores Internos, associado ao Audibra – Instituto dos Auditores Internos do Brasil) enfatiza o papel das boas práticas de governança em um contexto corporativo no qual a estratégia deve estar alinhada à missão da Companhia, através do encorajamento de ações proativas para o alcance das metas da organização, estabelecendo de forma clara e objetiva o gerenciamento de riscos e controles internos como responsabilidade da gestão. Os processos operacionais somente devem existir para que os esforços e recursos disponíveis sejam direcionados ao alcance dos objetivos estratégicos. Nesse sentido, as três linhas do modelo compreendem:

a. **1ª linha: gestão e supervisão** – o gerenciamento dos riscos e dos sistemas de controles internos de um determinado processo são atividades atribuídas aos gestores desse processo, inclusive com a aplicação de modelos de mercado;

b. **2ª linha: gestão especialista** – apoia, monitora e instrumentaliza a 1ª linha, integrando e orientando os vários esforços, em consonância com os objetivos estabelecidos pela Companhia;

c. **3ª linha: auditoria interna** – avalia, de forma independente, se as 1ª e 2ª linhas estão realizando suas atividades dentro das melhores práticas de governança corporativa. O Comitê de Auditoria Estatutário também faz parte da 3ª linha.



Fonte: *The Institute of Internal Auditors – Standards and Guidelines – North America, 2020*

5 PRINCÍPIOS

A PGERCI está alinhada com a missão, visão e valores éticos da Companhia, subsidiando o processo de planejamento estratégico e seus desdobramentos, com vistas ao cumprimento das leis e regulamentos aplicáveis; à eficácia e eficiência das operações; à consistência, tempestividade e proteção adequada das informações; à promoção de sinergia entre as áreas, bem como à salvaguarda dos ativos da empresa. São princípios da gestão de riscos e controles internos, baseados na norma ISO 31000:2018, e compartilhados pela Corsan:

a. **Criar e proteger valor:** realização de procedimentos de modo que os objetivos possam ser demonstrados e para uma melhoria de desempenho no que tange à segurança e saúde das pessoas, segurança patrimonial, conformidade legal e regulatória, aceitação pública, proteção ao meio ambiente, qualidade do produto final, gerenciamento de projetos, eficiência nas operações, governança e reputação;

b. **Ser parte integrante de todos os processos organizacionais:** a gestão de riscos deve ser levada em consideração no planejamento estratégico da empresa, como parte integrante de todos os processos organizacionais, mas sem deixar de ser atividade autônoma – ou seja, com estrutura própria e dedicada de funcionamento – separada das principais atividades e processos da empresa, mas não deixando de ser integrada a todos eles;

c. **Ser parte da tomada de decisão:** a organização necessita estabelecer maiores índices de segurança e confiabilidade de suas informações, priorizar as ações e distinguir entre formas alternativas de ação;

d. **Abordar explicitamente a incerteza:** a incerteza e a subjetividade fazem parte do gerenciamento de riscos – os meios pelos quais são tratadas devem ser explicitamente abordados;

e. **Ser sistemática, estruturada e oportuna**, contribuindo para a eficiência e para que os resultados sejam mais consistentes, comparáveis e confiáveis;

f. **Basear-se nas melhores informações disponíveis:** dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões e opiniões de especialistas, sempre levadas em consideração quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergência de opiniões de especialistas;

g. **Ser feita sob medida:** a gestão depende do tamanho, da necessidade e do apetite ao risco, alinhados com os contextos interno e externo da organização e com o perfil de cada risco;

h. **Considerar fatores humanos e culturais:** reconhecer as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização. Portanto, conhecimento e cultura organizacional são ferramentas utilizadas para aperfeiçoamento da gestão de riscos e controles internos, pois as pessoas são parte importante do processo;

i. **Ser transparente e inclusiva:** o envolvimento apropriado e oportuno das partes interessadas, e em particular dos tomadores de decisão em todos os níveis da organização, assegura que a gestão de riscos permaneça pertinente e atualizada. O envolvimento permite que os *stakeholders* sejam devidamente representados e tenham suas opiniões levadas em consideração na determinação dos critérios de risco;

6 DIRETRIZES

Os objetivos estratégicos definidos pela Administração devem considerar os riscos inerentes ao negócio, sendo que a PGERCI deve ser disseminada a todos os níveis hierárquicos da Companhia, promovendo a capacitação dos atores envolvidos na metodologia aplicada. Os riscos devem ser identificados, analisados, avaliados e mitigados, por meio da aplicação de controles adequados, conforme o processo de gestão de riscos e controles internos adotado pela Corsan, descrito com detalhes no Manual de Gestão de Riscos e Controles Internos, parte integrante desta política. Nessa esteira, a gestão de riscos e controles internos baseia-se nas seguintes diretrizes:

a. **fortalecimento das práticas de governança corporativa** na Corsan, baseadas no conceito das três linhas, facilitando a desenvolvimento contínuo da organização, no desenvolvimento de estratégias para promover a maturidade dos processos de governança da Companhia;

b. **identificação e avaliação dos riscos** associados ao não cumprimento das metas e objetivos da empresa, considerando a probabilidade de ocorrerem e os impactos sobre os negócios, caso se materializem;

c. **disseminação da cultura de gestão de riscos e controles internos** a partir da autoridade funcional de gestão de riscos e controles internos, devendo ser praticada em todos os níveis hierárquicos da Companhia, pela incorporação de seus princípios, de forma sistemática, nos processos de trabalho. A autoridade funcional de gestão de riscos e controles internos é a Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade (SUCORP), vinculada à Diretoria da Presidência;

d. **os empregados envolvidos com as atividades de gestão de riscos e controles internos devem ser capacitados**, pela autoridade funcional de gestão de riscos e controles internos, na metodologia adotada pela Companhia;

e. **a autoridade funcional de gestão de riscos e controles internos deve instituir políticas, normas e procedimentos**, assim como apoiar as unidades organizacionais na identificação, implementação e administração, de forma integrada, de controles internos eficazes e suficientes para mitigar os efeitos negativos dos riscos nos negócios da empresa;

f. **os profissionais da Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade devem ter acesso** facilitado a dados e informações, bem com dispor dos recursos necessários à plena execução de suas atividades, responsabilizando-se pela confidencialidade das informações utilizadas;

g. **o aperfeiçoamento da gestão de riscos e controles internos deve ocorrer por ciclos** de avaliações e revisões (monitoramento constante), e também em resposta a um fato específico (planos de contingência);

h. **a manutenção de sistemas e estruturas de controles internos alinhados com as melhores práticas**, os quais devem ser revisados e atualizados periodicamente, a fim de que eventuais deficiências sejam pronta e integralmente corrigidas, de forma a garantir sua efetividade.

7 COMPETÊNCIAS

7.1 Compete ao Conselho de Administração:

a. apreciar e aprovar a PGERCI e o Manual de Gestão de Riscos e Controles Internos, que serão revisados sempre que necessário ou, no mínimo, anualmente;
b. acompanhar o cumprimento da PGERCI;
c. incorporar as práticas de gestão de riscos e controles internos ao processo decisório;
d. apreciar e aprovar os relatórios de controles internos.

7.2 Compete ao Comitê de Auditoria Estatutário:

a. apreciar e manifestar-se sobre a PGERCI e o Manual de Gestão de Riscos e Controles Internos;
b. acompanhar o Plano Anual de Gestão de Riscos e Controles Internos e avaliar a efetividade dos procedimentos contidos no Plano;
c. supervisionar as atividades das 2ª e 3ª linhas, avaliando a exposição aos riscos e monitorando os controles internos, podendo requerer, sempre que necessário, informações detalhadas para subsidiar eventuais recomendações;
d. avaliar e monitorar os planos de ação de mitigação de riscos e a qualidade e integridade do sistema de controles internos da

Companhia, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias;

e. manifestar-se, previamente ao Conselho de Administração, a respeito dos relatórios de gestão de riscos e controles internos, como suporte à tomada de decisão.

7.3 Compete à Auditoria Interna – AUDIT

a. Auditar sistematicamente a existência, o cumprimento, e a eficácia da PGERCI e recomendar melhorias;
b. Auditar os riscos estratégicos e de negócio da organização, bem como seus controles internos;
c. Utilizar o Plano Anual de Gestão de Riscos Corporativos como subsídio ao Plano Anual de Auditoria Interna da Corsan;
d. Apoiar e supervisionar as atividades das 2ª e 3ª linhas, avaliando a exposição aos riscos e monitorando os controles internos, podendo requerer, sempre que necessário, informações detalhadas para subsidiar eventuais recomendações e pareceres.

7.4 Compete ao Diretor-Presidente:

a. avaliar a PGERCI e submetê-la à aprovação da Diretoria Colegiada, previamente à submissão ao Conselho de Administração;
b. garantir a incorporação das práticas de gestão de riscos e controles internos ao processo decisório;
c. propor à Diretoria Colegiada o Plano Anual de Gestão de Riscos e Controles Internos e, uma vez homologado, garantir o seu cumprimento;

d. garantir a avaliação e o monitoramento dos planos de ação de mitigação de riscos por parte de todas as unidades organizacionais da Corsan.

7.5 Compete à Diretoria Colegiada:

a. avaliar e aprovar a PGERCI;
b. incorporar as práticas de gestão de riscos e controles internos ao processo decisório;
c. aprovar o Plano Anual de Gestão de Riscos e Controles Internos;
d. avaliar e monitorar os planos de ação de mitigação de riscos;
e. assegurar os recursos necessários para a execução dos planos de ação de mitigação de riscos;
f. patrocinar a implantação de práticas de negócio eficientes e controles internos adequados e eficazes.

7.6 Compete ao Comitê Executivo de Riscos:

a. acompanhar o atendimento da PGERCI e do Plano Anual de Gestão de Riscos Corporativos;
b. subsidiar a Diretoria Colegiada na definição do apetite ao risco da Companhia;
c. avaliar os níveis de alçada de riscos, os quais definem as responsabilidades para aprovação e tratamento dos riscos;
d. identificar e analisar os controles internos nas áreas que representam, visando avaliar sua eficácia, suficiência e aplicabilidade na mitigação os riscos aos quais estão relacionados;
e. acompanhar a implantação dos planos de ação mitigatórios dos riscos corporativos;

f. identificar, construir e acompanhar os indicadores-chave de risco (*KRIs - Key Risk indicators*) e acompanhar os indicadores- chave de performance (*KPIs - Key Performance Indicators*), buscando sempre utilizar ambos os conjuntos de indicadores como ferramentas de gestão de riscos e controles internos;
g. avaliar a matriz de riscos e de controles internos, mantendo-as sempre atualizadas e visando sempre aprimoramentos constantes.

7.7 Compete à Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade - SUCORP:

A Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade é responsável por constituir e aplicar ferramentas e mecanismos de gestão de riscos e controles internos adequados à aplicação desta Política, mensurar e avaliar a qualidade destes mecanismos, além de elaborar e submeter proposta de revisão anual desta Política, ou sempre que necessário.

7.8 Compete às demais unidades organizacionais:

a. Conhecer e aplicar a PGERCI e o Plano Anual de Gestão de Riscos;
b. Identificar, analisar, avaliar, tratar e monitorar os riscos corporativos de sua competência;
c. Traçar os planos de ação de mitigação de riscos corporativos de sua competência;
d. Apresentar à Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade, o tratamento e os planos de ações de mitigação de riscos de sua competência;

e. Acompanhar a evolução dos planos de ação de mitigação de riscos corporativos de sua competência;
f. Definir os indicadores de riscos corporativos e fazer o seu acompanhamento;
g. Estabelecer, manter, promover e avaliar as práticas de negócio eficientes e controles internos adequados e eficazes;
h. Documentar os controles internos implementados nas áreas de negócio;
i. Apresentar à Superintendência de Governança Corporativa, Gestão de Riscos e Conformidade, a documentação dos controles internos implantados na área de sua competência;
j. Definir os indicadores dos controles internos e fazer o seu acompanhamento.

8 DISPOSIÇÕES FINAIS

Este documento deverá ser revisado e aprovado pela Diretoria Colegiada e pelo Conselho de Administração.

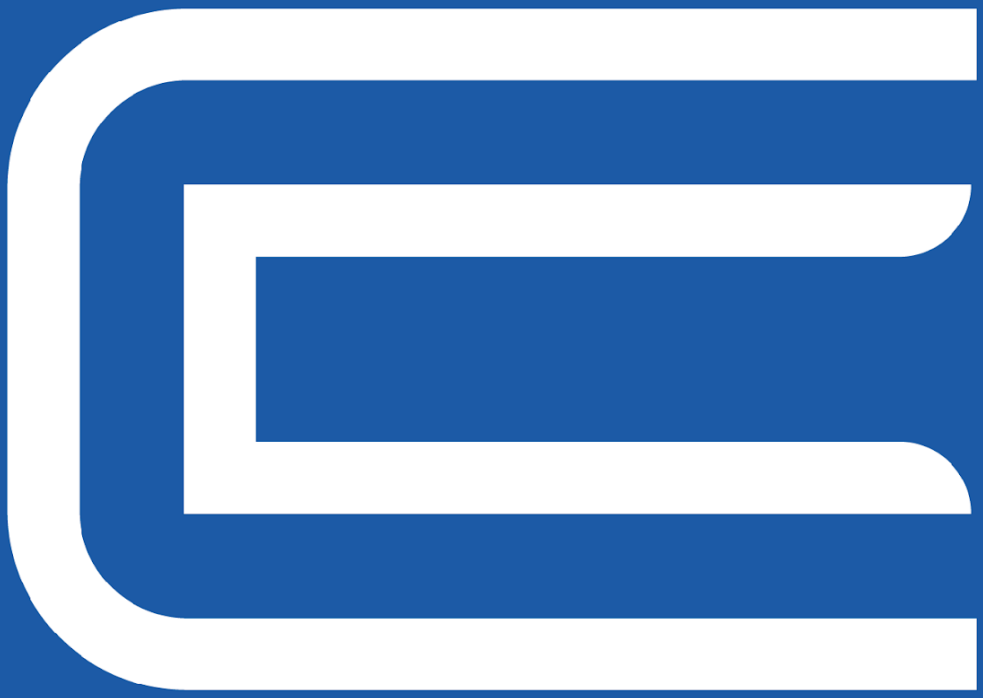
9 REFERÊNCIAS

- Modelo internacional COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management) - Framework 2004
- *The Institute of Internal Auditors – Standards and Guidelines* (O Instituto dos Auditores Internos – Padronização e Orientação) – América do Norte, 2020
- Regulamento do Novo Mercado da B3;
- ABNT NBR ISO 31000:2018;
- ABNT NBR GUIA 73:2009.

- Assi, Marcos. *Gestão de riscos com controles internos: ferramentas, certificações e métodos para garantir a eficiência dos negócios* | São Paulo: Saint Paul Editora, 2013.

10 ANEXOS

10.1 Manual de Gestão de Riscos e Controles Internos



corsan

COMPANHIA RIOGRANDENSE DE SANEAMENTO – CORSAN
Rua Caldas Júnior, 120 / 18º andar
CEP 90010-260 – Porto Alegre – RS
www.corsan.com.br