Política de Gestão de Riscos e Controles Internos

POL_DGC_0008

Objetivo: Definir as diretrizes e a metodologia para a Gestão de Riscos na Associação Administradora da Faixa de 3,5 GHZ – EAF, em atendimento às leis e regulamentações aplicáveis, definindo papéis e responsabilidades que assegurem a correta identificação e tratamento dos potenciais de riscos corporativos. Estabelecer as diretrizes e estruturas de controles internos, a fim de garantir que sejam efetivos e consistentes com a natureza, complexidade e riscos das operações, garantindo que os objetivos da EAF sejam alcançados.
Autor do documento: Diretoria de Governança e Compliance
Contato: Gerência de Compliance
Abrangência: Todos os colaboradores da EAF.

Sumário

1 – Objetivo

Definir as diretrizes e a metodologia para a Gestão de Riscos na Associação Administradora da Faixa de 3,5 GHZ – EAF, em atendimento às leis e regulamentações aplicáveis, definindo papéis e responsabilidades que assegurem a correta identificação e tratamento dos potenciais riscos corporativos. Estabelecer as diretrizes e estruturas de controles internos, a fim de garantir que sejam efetivos e consistentes com a natureza, complexidade e riscos das operações, garantindo que os objetivos da EAF sejam alcançados.

2 – Abrangência

Aplica-se a todos os colaboradores e processos inerentes à operação da EAF.

3 – Definições

EAF: Associação Administradora da Faixa de 3,5 GHZ.

Controles internos: Políticas, normas, processos, indicadores e procedimentos criados com o objetivo de proporcionar um grau de confiança razoável na eficácia e eficiência das operações, nos relatórios e informes, e no cumprimento das exigências regulatórias, que apoiem a EAF no atingimento de seus objetivos e obrigações. Compreende todas as ações tomadas suportadas pelos valores da organização, de economicidade, modicidade, eficiência, probidade administrativa e ética, declarados no seu estatuto.

Evento: Incidente ou ocorrência, a partir de fontes internas ou externas à EAF, capaz de afetar a realização dos seus objetivos.

Gestão de Riscos: É o conjunto de ações coordenadas e direcionadas ao desenvolvimento, implantação e disseminação de metodologia de mapeamento de riscos, de quaisquer naturezas, internos ou externos, que compreendam as etapas de identificação, análise, priorização e tratamento destes riscos, com periodicidade definida.

Impacto: São as consequências da ocorrência do evento.

Key Performance Indicator (KPI): Significa Indicador Chave de Desempenho e tem por finalidade medir a etapa de um processo ou sistema, com acompanhamento periódico dos resultados, apoiando na avaliação e identificação de vulnerabilidades ou riscos.

Matriz e Mapa de Riscos: Visões consolidadas dos riscos, já mensurados em níveis de impacto e probabilidade, que auxiliam na comparação e priorização do tratamento dos riscos. A matriz e o mapa de riscos estão em constante atualização, de acordo com a evolução interna da organização e dos cenários externos que afetam suas atividades.

Modelo das Três Linhas: Modelagem, instituída pelo IIA (The Institute of Internal Auditors), que enfatiza o papel das boas práticas de governança, no qual a estratégia deve estar alinhada à missão da Companhia, através do encorajamento de ações proativas, estabelecendo de forma clara e objetiva o gerenciamento de riscos e controles internos como responsabilidade da gestão. O modelo determina papéis e responsabilidades sobre as três linhas, que devem atuar de maneira harmônica, porém independentes entre si.

Plano de Ação: É a definição das ações corretivas para reduzir a exposição aos riscos residuais, a partir da identificação das deficiências ao longo do ciclo de avaliação do ambiente de controles internos.

Probabilidade: São as chances de ocorrer um determinado evento.

Risco: Possibilidade de um evento ocorrer e ter impacto nos objetivos da organização, sendo medido em termos de impacto e probabilidade. O risco pode ter origem interna (inerente a processos da própria organização) ou externa (fatores externos que afetam os objetivos da organização), e são agrupados em categorias distintas, de forma a facilitar seu entendimento.

Stakeholders: São as partes interessadas da EAF, ou seja, ANATEL, GAISPI e Associadas.

Tipos de Controles: Os controles internos dos processos de negócio podem ser classificados em Preventivo (Executados no início do processo - previnem o acontecimento de erros ou irregularidades e minimizam os riscos na fonte) e Detectivo (Executados ao longo do processo, detectam erros que são difíceis de definir ou prever). Também podem ser classificados como Manual (realizado por meio de conferências ou procedimentos executados por uma pessoa) e Automático (validações executadas por sistemas com pouca ou nenhuma interferência de pessoas).

5 – Documentos de Referência

Código de Ética e Conduta da EAF;

Regimento Interno da EAF;

COSO ERM;

ISO 31000:2018; e

Modelos das Três Linhas do IIA.

6 – Autoridade e Responsabilidade

6.1. Diretorias da EAF

Identificar os riscos relacionados às suas atividades, de origem interna ou externa;

Avaliar os inputs de demais áreas e outros canais da organização que podem apoiar na identificação de novos riscos;

Realizar a análise e a categorização dos riscos;

Revisar, conforme a metodologia, os níveis de impacto e probabilidade dos riscos;

Aprovar a Política de Gestão de Riscos da EAF e suas futuras revisões;

Aprovar o mapa de riscos e a priorização dos riscos a serem tratados;

Definir ou validar os responsáveis (“risk owners”) para cada um dos riscos mapeados.

6.2. Grupos de Trabalho de Riscos

Definir o tratamento a ser dado a cada um dos riscos (evitar, transferir, mitigar ou aceitar);

Aprovar o plano de ação de resposta e tratamento dos riscos;

Propor melhorias no processo de gerenciamento de riscos da EAF;

Definir e apresentar o plano de ação de resposta aos riscos sob sua responsabilidade;

Implantar o plano de ação e controles internos necessários;

Revisar os riscos e suas variáveis periodicamente.

6.3. Diretoria de Governança e Compliance

Desenvolver, aplicar e disseminar a metodologia de gestão de riscos da EAF;

Promover a cultura de gestão de riscos junto às demais diretorias;

Coordenar as atividades de todas as etapas do ciclo de mapeamento de riscos;

Apoiar os gestores das áreas na definição dos planos de ação para tratamento dos riscos;

Apresentar em REDIR o planejamento anual do mapa de riscos, e a evolução das etapas de identificação, análise, mensuração e tratamento dos riscos.

7 – Gestão de Riscos

As atividades de Gestão de Riscos devem ser constantemente avaliadas, tomando como referência as práticas de Governança Corporativa definidas pelo COSO ERM: 2017 – Gerenciamento de Riscos Corporativos Integrado com estratégia e Performance e pela ISO 31000:2018 – Risk Management Guidelines.

A EAF adota modelo de gestão de riscos baseado nos conceitos das Três Linhas instituída pelo IIA (The Institute of Internal Auditors), sendo:

- Primeira linha: representada por gestores das áreas na Diretoria Corporativa, Diretoria de Comunicação, e Diretoria de Operações, os quais devem assegurar a efetiva gestão de riscos dentro do escopo das suas responsabilidades diretas;

- Segunda linha: refere-se às áreas de controle da organização, sendo responsável por apoiar e monitorar, bem como suportar a Primeira Linha, fornecendo capacitação e apoio técnico no modelo de Gestão dos Riscos e Controles Internos;

- Terceira linha: composta pelas diversas auditorias, atuando de forma independente e objetiva, tem como sua atividade principal fornecer opiniões imparciais à Diretoria de Governança e à Diretoria Geral sobre o processo de gerenciamento de riscos e a efetividade dos controles internos.

A metodologia de gestão de riscos da EAF compreende as etapas de Identificação, Análise, Mensuração, Priorização, Tratamento e Monitoramento dos Riscos.

7.1. Identificação dos Riscos

A identificação, ou revisão dos riscos já identificados, é realizada anualmente, mas pode ter sua frequência aumentada conforme as necessidades da EAF.

O processo de identificação dos riscos envolve uma entrevista individualizada junto a todos os diretores e demais stakeholders da EAF, além da utilização de evidências coletadas através dos Controles Internos, Auditorias, e canais de comunicação da organização, como Atendimento, Canal de Denúncias, e outros. Todas as entrevistas são coordenadas e realizadas pela Diretoria de Governança e Compliance.

Os riscos serão categorizados, a princípio, nos seguintes grupos:

Riscos de origem externa:

- **Econômico** – Riscos associados a políticas econômicas, como câmbio e taxa de juros, volatilidade do mercado, incidentes de logística internacional, escassez de insumos e concentração de fornecedores;
- **Legal** – Riscos referentes a novas obrigações regulatórias ou regulamentações trabalhistas;

- **Natural** – Riscos vinculados a epidemias e desastres naturais de grande magnitude;
- **Político** – Riscos relacionados a alterações de políticas públicas, tensões geopolíticas, conflitos internacionais e outros, que tenham o potencial de afetar as atividades da EAF;
- **Sociocultural** – Pressões exercidas pela sociedade, como pautas sociais e ambientais restritivas, greve geral, e outros;
- **Tecnologia** – Riscos associados à evolução tecnológica, ataques cibernéticos externos.

Riscos de origem interna:

- **Ambiental**: Riscos referentes a multas ambientais, gestão de resíduos, destinação de materiais e equipamentos obsoletos;
- **Financeiro**: Riscos vinculados à falta de recursos financeiros, perdas na cadeia de pagamentos e fraudes;
- **Governança**: Riscos relacionados a desvios de conduta, danos a reputacionais, não cumprimento de obrigações regulatórias, fraudes contratuais, sucessão de executivos, relacionamento com associadas e não conformidades;
- **Operacional**: Riscos que abrangem todas as etapas dos processos operacionais, desde falhas no planejamento e gestão dos projetos, erros de projeção de demanda, gestão de estoques e falhas na prestação de serviços terceirizados;
- **Pessoal**: Riscos relacionados à equipe reduzida, falha humana, defasagem de conhecimento técnico, cultura organizacional e segurança do trabalho;
- **Regulação**: Riscos referentes a sanções tributárias, ações cíveis e contencioso trabalhista;
- **Tecnologia**: Riscos vinculados a incidentes de segurança de informação, violação de dados pessoais de colaboradores ou clientes e indisponibilidade sistêmica.

Novas categorias de risco podem ser adicionadas à matriz, de acordo com a necessidade da organização e a identificação de novos cenários internos ou externos que afetem suas atividades.

7.2. Análise dos Riscos

A etapa de análise envolve o estudo de causas, fatores e consequências dos riscos, e demanda o conhecimento técnico adequado, que suporte a adequada categorização e apoie na estimativa de mensuração destes riscos, nos eixos de impacto e de probabilidade de materialização.

7.3. Mensuração dos Riscos

Para a etapa de mensuração, todos os riscos, já categorizados, deverão ser classificados em níveis de impacto e de probabilidade, para posterior enquadramento no mapa de riscos. Esta classificação possui a finalidade de auxiliar a Alta Direção na priorização e tratamento dos riscos.

Os níveis de impacto, além da magnitude financeira, podem estar alinhados a aspectos estratégicos, ou também reputacionais e de exposição, e possuem as seguintes escalas:

- 5 – Muito Alto
- 4 – Alto
- 3 – Médio
- 2 – Baixo
- 1 – Muito Baixo

Os níveis de probabilidade devem considerar a possibilidade, em termos percentuais, da materialização do risco, coerente com a malha de controles internos existentes na organização, e estão divididos nas seguintes escalas:

- 5 – Iminente (maior que 80%)
- 4 – Muito Provável (maior que 60% até 80%)
- 3 – Provável (maior que 40% até 60%)
- 2 – Pouco Provável (maior que 20% até 40%)
- 1 – Improvável (até 20%)

Atribuídos os níveis de impacto e probabilidade, e multiplicando-se os dois fatores, gera-se uma resultante com a nota de risco, conforme visão gráfica a seguir:

A obtenção da "nota de risco" possibilita sua organização na matriz e mapa de riscos, por níveis de criticidade, e consequente priorização para seu tratamento.

7.4. Priorização dos Riscos

Todos os riscos mapeados, conforme a metodologia, terão como resultante uma pontuação que deve ser utilizada como base para a priorização de seu tratamento.

Os riscos com as respectivas pontuações são revisados por todos os Diretores. Após essa revisão, somente os riscos classificados com alta pontuação (maior que 10) são levados para priorização, por meio de votação eletrônica por todos os Diretores.

Nessa reunião de priorização é definida a quantidade de riscos a serem trabalhados no próximo ano.

7.5. Tratamento dos Riscos

Para todos os riscos priorizados são definidos os responsáveis e os grupos de trabalho que ajudarão no tratamento do respectivo risco.

Os grupos de trabalho terão reuniões periódicas com a Diretoria de Governança e Compliance para que sejam identificadas as causas, consequências e definido o tratamento a ser dado para cada risco.

As medidas de tratamento podem ser:

Evitar: O risco pode ser evitado quando se realiza um trabalho efetivo nas suas causas, ou também revisando o planejamento e processos operacionais de forma que a condição que favorece a existência do risco seja eliminada. A escolha por esta estratégia pode demandar a implantação de controles internos e indicadores que assegurem sua efetividade.

Transferir: Envolve encontrar uma terceira parte que esteja disposta a assumir a gestão do risco, sua resposta e sua eventual materialização. Esta estratégia de resposta pode ser eficaz em eventuais riscos com exposição financeira, e normalmente envolve um contrato ou remuneração à uma terceira parte para que esta assuma este risco.

Mitigar: A mitigação busca reduzir os níveis de impacto e/ou probabilidade de um risco até que se alcance um nível aceitável. Em geral, tomar as ações necessárias previamente é mais eficaz do que reparar as consequências da materialização de um determinado risco. A decisão pela estratégia de mitigação exige um esforço da organização, através da implantação de controles internos adequados, que se desdobram em evoluções em processos e sistemas, confecção de indicadores, apoio externo, e adequação de força de trabalho.

Aceitar: Para os riscos de origem interna, a estratégia de aceitar o risco pode ser adotada nas situações em que seja inviável, tecnicamente ou financeiramente, a utilização de outra estratégia. Já nos casos de risco de origem externa, a estratégia pode ser adotada em casos de baixa influência da organização na gestão desses riscos. Não obstante, a organização tem a possibilidade de lançar mão de planos de contingência, planejados com antecedência, na eventual ocorrência destes riscos.

7.6. Monitoramento dos Riscos

O monitoramento dos riscos é realizado com a finalidade de comprovar a adequação e a efetividade dos Controles Internos, através de avaliações contínuas e isentas, conduzidas pela Diretoria de Governança e Compliance. Esta etapa engloba a avaliação de indicadores, planos de ação e demais aspectos relacionados aos riscos mapeados.

7.7. Comunicação dos Riscos

A comunicação clara e objetiva a todas as partes interessadas, em todas as etapas do gerenciamento de riscos é de fundamental importância para o bom funcionamento do processo, e proporciona a conscientização sobre a importância de uma cultura de gestão de riscos na organização.

8 – Controles Internos

A EAF adota as melhores práticas de Governança Corporativa utilizando metodologias de controles internos para assegurar que os riscos inerentes às atividades da organização sejam identificados e administrados adequadamente.

A EAF possui controles internos voltados para suas atividades e seus sistemas de informações financeiras, operacionais e gerenciais, garantindo a confiabilidade das informações, a utilização eficiente dos recursos e o cumprimento da legislação e documentos internos da organização.

O gerenciamento de riscos se concentra na identificação de ameaças e oportunidades, mas são os Controles Internos que ajudam a combater as ameaças e aproveitar as oportunidades identificadas. Por esse motivo é que controle interno e gestão de riscos devem andar juntos.

Desta forma, as descrições dos controles internos devem ser acessíveis a todos os colaboradores e compreender ações contínuas relativas a suas atividades, operações e níveis hierárquicos, prevendo, no mínimo:

a) A definição dos objetivos dos controles e das responsabilidades da organização, de forma a evitar conflito de interesses nos processos internos;

b) Os meios de identificação e avaliação de riscos que podem ameaçar sua eficácia;

c) Canais de comunicação que assegurem aos colaboradores o acesso às informações relevantes para execução das suas tarefas e responsabilidades, bem como o encaminhamento de contribuições para seu aperfeiçoamento;

d) Existência de testes de segurança e conciliação para os sistemas de informações, em especial aqueles mantidos em meio eletrônico;

e) Ações ou planos de contingência, quando necessários.

8.1. Avaliação de Controles Internos

A avaliação está sob responsabilidade da Diretoria de Governança e Compliance e tem como objetivo a compreensão do mapeamento dos processos de cada área, obtendo uma visão geral de como os controles funcionam, avaliar a eficácia dos controles identificados, confirmar se estão em operação, revisar os riscos dos processos e identificar novos riscos, levantar evidências da eficiência dos controles existentes e registrar os resultados na Matriz de Controles Internos.

Estão apresentados a seguir os conceitos a serem considerados como resultado da avaliação:

- Controles Não Implementados: Os controles internos apresentam falta de confiabilidade e as ações corretivas são implementadas somente dos riscos.
- Controles Implementados: Os controles internos apresentam confiabilidade, não necessitando de ações corretivas. Além disso, existem políticas, normas, procedimentos formalizados.

Para os controles considerados Não Implementados, a Diretoria de Governança e Compliance deverá registrar as deficiências de controles, abrindo o registro de deficiências, para que as áreas envolvidas elaborem Planos de Ação corretivos.

A avaliação de Controles Internos ocorre em duas etapas:

Testes de Desenho: Consistem em avaliar se o controle existe e devem ser realizados por meio de indagação, observação e análise de documentação.

Testes de Efetividade: Consistem em avaliar a efetividade do funcionamento dos controles e devem ser realizados por meio de análise de documentação ou reperformance, com base em seleção de amostras aleatórias, para garantir a confiabilidade da base, sendo que o tamanho da amostra deve ser definido de acordo com a frequência do controle conforme abaixo:

Natureza do Controle	Frequência de Execução	Tamanho da Amostra
Manual	Muitas vezes ao dia	25
Manual	Diário	15
Manual	Semanal	5
Manual	Mensal	2
Manual	Trimestral	1
Manual	Annual	1
Controle Automático	Testar uma amostra de cada controle automatizado	

Para a execução dos testes será necessário avaliar se o controle é executado corretamente de acordo com: desenho, frequência esperada, se é aplicado a todas as operações

contempladas pelo fluxo operacional e revisar se os desvios estão suportados por controles compensatórios.

Os Testes de Controles Internos serão avaliados por meio de:

Indagação: Entrevistas detalhadas para obtenção de evidências quanto à eficácia dos controles. Esta técnica deve ser realizada, obrigatoriamente, em conjunto com outras técnicas de execução de testes (exemplo: análise de evidência documental), para corroborar a informação obtida na indagação.

Observação: Consiste em observar a execução de uma atividade de controle, o que normalmente fornece evidência substancial sobre sua eficácia. Apesar disso, por si só, não fornece evidência suficiente para concluir sobre a eficácia da atividade de controle. A ausência de erros nos itens observados não fornece evidência conclusiva de que a atividade de controle é eficaz, sem a supervisão.

Análise de Documentação: Obtenção de evidências quanto à eficácia do controle por meio de análise da documentação. O grau de segurança que se obtém com esta técnica é considerado alto para a grande maioria dos controles, porém pode haver a necessidade de ser complementado com outro tipo de técnica.

Reperformance: Consiste na reexecução independente do controle. O resultado confere alta segurança quanto à efetividade do controle para a amostra selecionada. Esta técnica tem como ponto desfavorável o seu alto custo e tempo para execução.

Os testes de controle serão documentados conforme periodicidade e metodologia definida em relatório e apresentado à Alta Administração para ciência da efetividade dos controles existentes.

A tabela de referência a seguir auxilia a avaliação da vulnerabilidade do ambiente de controle interno

Matriz de Avaliação de Vulnerabilidade de Controles Internos

Relevância			Implementação			Histórico	
Baixa	Processos suporte de baixo impacto na operação da EAF.	+	**Baixa**	Controles internos implementados em sua maioria (acima de 80%).	+	**Baixa**	Sem incidência de falhas ou ocorrências. Incidência não significante.
Média	Processos suporte que impactam a operação da EAF.		**Média**	Controles internos parcialmente implementados (50% à 80%).		**Média**	Baixa incidência de falhas ou ocorrências.
Alta	Processos estratégicos que impactam a operação da EAF.		**Alta**	Controles internos não implementados (abaixo de 50%).		**Alta**	Alta incidência de falhas ou ocorrências.

A avaliação final do nível de vulnerabilidade encontrado, om resultante “baixa”, “média” ou “alta”, leva em consideração os três eixos descritos na tabela.

8.2. Identificação das deficiências

As deficiências são apontamentos, identificadas pela área responsável do processo ou pela Diretoria de Governança e Compliance, que demandam ação do responsável para correção da ocorrência, podendo decorrer, por exemplo, da ausência de controle, ausência de evidência na execução do controle, não aderência a uma norma aplicável ou não execução efetiva de um controle.

Nesta etapa, a identificação das deficiências pode ser realizada por qualquer membro da 1ª ou 2ª linha de defesa. A área responsável pelo processo, para o qual foi apontada uma deficiência, é responsável por apresentar como resposta uma proposta de solução, traduzida em um Plano de Ação.

9 – Orientações Gerais

Esta política contribui para que a EAF alcance os seus objetivos, através da implantação de mecanismos preventivos e de uma cultura organizacional de gestão de riscos, que são parte integrante de um modelo de governança ético e responsável.

Quaisquer dúvidas ou esclarecimentos deverão ser sanados junto à Diretoria de Governança e Compliance.

10 – Controle de Versionamento

Código	Data da Vigência	Motivo da Elaboração/Revisão	Elaborado por	Revisado por	Aprovado por
POL_DGC_0007	02/10/2023	Implantação	Dalton Pallopito	Silvio Starling e Vívian Fluminense	Diretoria EAF