Gestão de Compliance

Relatório de Análise de Compliance

PRJC21003

Auditoria de Incidentes e Requisições - 1º semestre 2021

Emissão: 06/08/2021 10:57

ATENÇÃO

As informações contidas neste documento são direcionadas aos usuários do sistema **Módulo Risk Manager©**, desenvolvido pela **Modulo Security Solutions S/A.**

Caso não tenha autorização de acesso a essas informações, saiba que sua leitura, divulgação ou cópia são proibidas. O uso impróprio será tratado pela legislação em vigor com base nos acordos de sigilo.
A reprodução não autorizada, em todo ou em parte, poderá resultar em punições civis e criminais.

Modulo Security Solutions S/A
www.modulo.com.br
suporteriskmanager@modulo.com.br

1. RESUMO DA ANÁLISE

Este relatório apresenta o resultado da análise de *compliance* realizada no projeto Auditoria de Incidentes e Requisições - 1º semestre 2021. As investigações foram realizadas em macroprocessos (componentes de negócio estratégicos), sistemas organizacionais (componentes de negócio táticos), ativos e pessoas da Organização que tiverem sido incluídos no escopo do projeto como objetos da análise. Podem ter sido utilizados diversos métodos de verificação de evidências, tais como: análise de documentos, entrevistas, vistorias às instalações, dentre outros.

Algumas das principais questões tratadas aqui são:
(i) Quais os resultados obtidos na análise de *compliance*?
(ii) Quais os principais índices de *compliance* obtidos?
(iii) Como priorizar as ações de tratamento?

1.1 Análise do(s) documento(s) de referência

A análise identificou 1 documento(s) de referência total ou parcialmente atendido(s), representando 100,00% do total de 1 documento(s) investigado(s). De forma complementar, a análise identificou 0 documento(s) de referência não atendido(s), o que representa 0,00% do total investigado. Vale ressaltar que quanto maior for este segundo valor, maiores são os riscos de não aprovação em uma auditoria oficial. A Tabela 1 apresenta os resultados finais obtidos para cada documento de referência:

Documentos de referência	Requisitos Analisados	Compliance Index	Nível de Compliance	Nível de Compliance Index
Processo de Gerenciamento de Incidentes	8	68,75%	Parcialmente Atendido	Alta
Total	8	68,75%	Parcialmente Atendido	Alta

Tabela 1 – Documentos de referência - resultados finais

1.2 Análise dos requisitos

A análise identificou 8 requisito(s) total ou parcialmente atendido(s), representando 100,00% do total de 8 requisitos investigados. De forma complementar, a análise identificou 0 requisito(s) não atendido(s), o que representa 0,00% do total investigado. Vale ressaltar que quanto maior for este segundo valor, maiores são os riscos de não aprovação em uma auditoria oficial. A Figura 1 apresenta a distribuição dos requisitos por Nível de *Compliance* - para o resultado final e para cada documento de referência analisado:

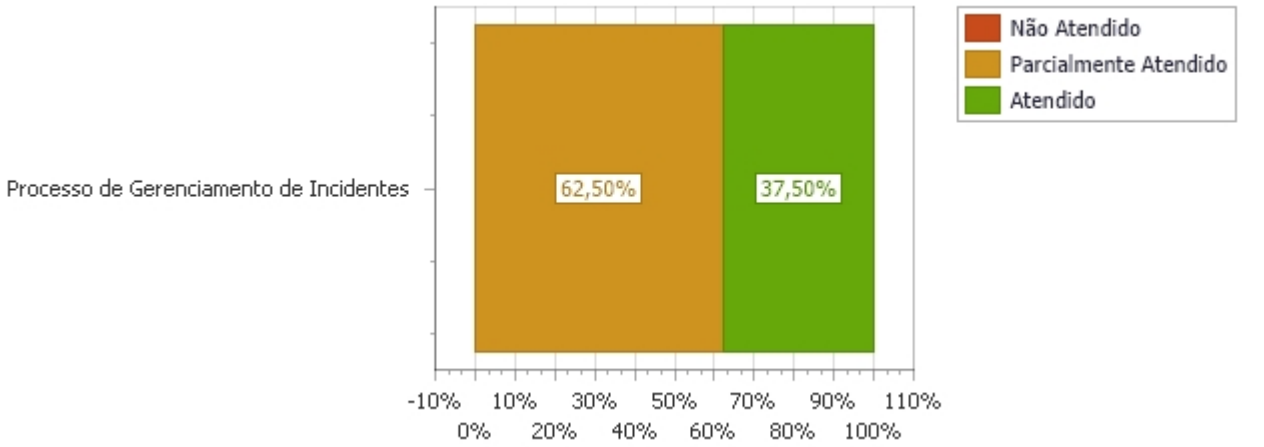

Figura 1 - Requisitos - distribuição por Nível de *Compliance*

OBSERVAÇÃO: Todos os requisitos existentes no(s) documento(s) de referência avaliado(s) foram considerados no gráfico acima, incluindo os que existem apenas para agrupar requisitos em níveis inferiores.

A Tabela 2 garante uma visão mais detalhada, apresentando a relação TOP 10 dos requisitos por *Compliance Index*. São mostrados os resultados consolidados em visões quantitativa (*Compliance Index*) e qualitativa (Nível de *Compliance*). Para uma relação completa dos requisitos analisados, veja a Tabela 6.

Documentos de Referência	Requisitos	Compliance Index	Nível de Compliance	Nível de Compliance Index
Processo de Gerenciamento de Incidentes	Atribuir chamado ao fornecedor	100,00%	Atendido	Muito Alta
Processo de Gerenciamento de Incidentes	Categorizar chamado e Classificar como "Serviço Não Catalogado"	100,00%	Atendido	Muito Alta
Processo de Gerenciamento de Incidentes	Tomar ciência	100,00%	Atendido	Muito Alta
Processo de Gerenciamento de Incidentes	Contatar o usuário para fechar o chamado	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Iniciar atendimento pela área e investigar solução	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar incidente como resolvido e avaliar necessidade de requisição vinculada	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar incidente como resolvido e avaliar nova entrada na base de conhecimento	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar RESOLVIDO e avaliar nova entrada na base de conhecimento	50,00%	Parcialmente Atendido	Média

Tabela 2 - Requisitos com melhor desempenho de Compliance Index

Abaixo, a Tabela 3 apresenta a relação dos dez requisitos com pior desempenho por *Compliance Index* e seus respectivos Níveis de *Compliance*.

Documentos de Referência	Requisitos	Compliance Index	Nível de Compliance	Nível de Compliance Index
Processo de Gerenciamento de Incidentes	Contatar o usuário para fechar o chamado	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Iniciar atendimento pela área e investigar solução	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar incidente como resolvido e avaliar necessidade de requisição vinculada	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar incidente como resolvido e avaliar nova entrada na base de conhecimento	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Registrar RESOLVIDO e avaliar nova entrada na base de conhecimento	50,00%	Parcialmente Atendido	Média
Processo de Gerenciamento de Incidentes	Atribuir chamado ao fornecedor	100,00%	Atendido	Muito Alta
Processo de Gerenciamento de Incidentes	Categorizar chamado e Classificar como "Serviço Não Catalogado"	100,00%	Atendido	Muito Alta
Processo de Gerenciamento de Incidentes	Tomar ciência	100,00%	Atendido	Muito Alta

Tabela 3 – Os dez requisitos com pior desempenho de Compliance Index

1.3 Análise dos objetos

A análise identificou 1 objeto(s) cujos requisitos relacionados estão total ou parcialmente atendidos, representando 100,00% do total de 1 objetos investigados. De forma complementar, a análise identificou 0 objeto(s) cujos requisitos relacionados não estão atendidos, o que representa 0,00% do total investigado. Vale ressaltar que quanto maior for este valor, maiores são os riscos de não se passar em uma auditoria oficial. A Figura 2 apresenta a distribuição dos objetos por Nível de *Compliance*:

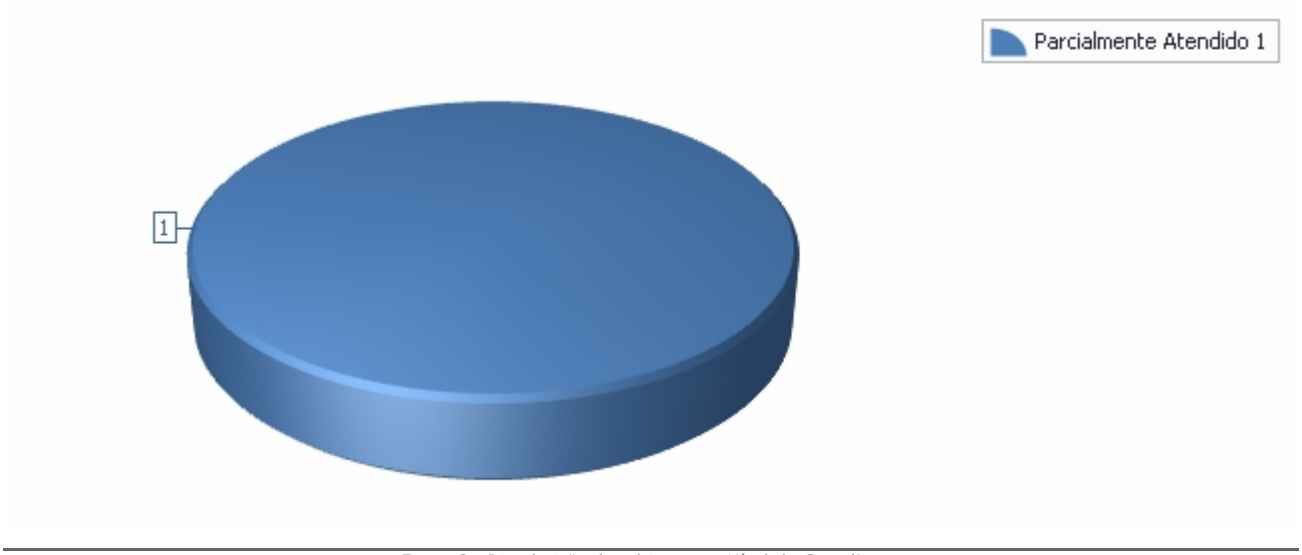

Figura 2 - Distribuição dos objetos por Nível de *Compliance*

A tabela 4 garante uma visão mais detalhada, apresentando a relação TOP 10 dos objetos por *Compliance Index* e seus respectivos Níveis de *Compliance*.

Objetos	Compliance Index	Nível de Compliance	Nível de Compliance Index
Gestão de Incidentes e Requisições	80,00%	Parcialmente Atendido	Alta

Tabela 4 - Objetos com melhor desempenho de Compliance Index

Abaixo, a Tabela 5 apresenta a relação dos dez objetos com pior desempenho por *Compliance Index* e seus respectivos Níveis de *Compliance*.

Objetos	Compliance Index	Nível de Compliance	Nível de Compliance Index
Gestão de Incidentes e Requisições	80,00%	Parcialmente Atendido	Alta

Tabela 5 – Os dez objetos com pior desempenho de Compliance Index

2. METODOLOGIA ADOTADA

O **Módulo Risk Manager** é um sistema de informação que automatiza o processo de gestão de *compliance* com base na análise de objetos, tais como ativos tecnológicos (*software* e equipamentos), não tecnológicos (pessoas, processos e ambientes) e componentes de negócio. A metodologia **GRC Metaframework** utilizada é exclusiva da **Modulo Security Solutions S/A** e está em conformidade com as diretrizes fornecidas pelas normas ISO 31000 e ISO Guia 73.

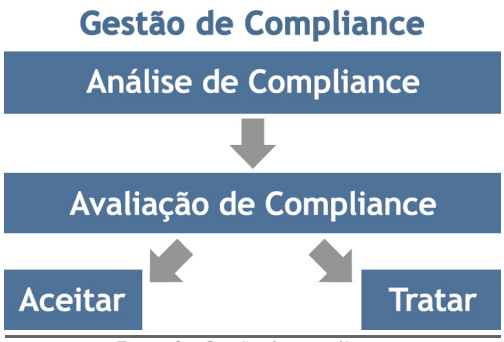

Figura 3 - Gestão de *compliance*

O *compliance* é calculado com base em dois índices distintos e complementares (*Compliance Index* e Nível de *Compliance*), a partir de uma ampla base de conhecimento atualizada. Dessa forma, a utilização do sistema proporciona aumento de produtividade, maior controle e padronização das atividades, aulixiando a Organização a obter os resultados desejados.

Figura 4 - GRC Metaframework

Os cabeçalhos das tabelas 6, 8, 9 e 10 são referenciados conforme a legenda abaixo:

No. Req	Número de Requisitos		
Qtd Perg	Quantidade de Perguntas	**PA**	Parcialmente Atendido
AT	Atendido	**NA**	Não Atendido

2.1 Índices de *Compliance*

Em função das exigências do mercado, governo, agências reguladoras e clientes, conhecer e avaliar a conformidade deixou de ser uma necessidade técnica e se tornou uma questão estratégica para as organizações.

Para fornecer a estimativa da conformidade, o sistema **Módulo Risk Manager** utiliza os seguintes índices:

Compliance Index (visão quantitativa) - representa o percentual de aderência das práticas organizacionais em relação às orientações descritas nos documentos de referência. É calculado para cada pergunta nas entrevistas de *compliance*, de acordo com as escalas de resposta utilizadas, e consolidado para requisitos, documentos de referência e objetos. Este índice é expresso em números percentuais e pode variar de 0 a 100%.

É importante observar que quanto maior o valor do *Compliance Index*, mais as práticas organizacionais estarão em conformidade com as exigências e as orientações dos documentos de referência.

Nível de *Compliance* (visão qualitativa) - representa o nível de atendimento de uma determinada pergunta conforme as evidências encontradas (podendo ser controles, documentos, práticas etc.) e consolidado em diversos níveis (requisito, documento de referência e objeto). Representa, em última análise, a interpretação dos valores calculados de *Compliance Index* e é expresso pelas opções Não Atendido, Parcialmente Atendido e Atendido.

Vale ressaltar que quanto maior for a quantidade de Níveis de *Compliance* "Não Atendido", maiores são os riscos de não se passar em uma auditoria oficial.

3. LIMITAÇÕES EXISTENTES

Os resultados encontrados baseiam-se nas pesquisas de *compliance* existentes no **Módulo Risk Manager**. Esses resultados devem ser utilizados como insumo, permitindo que o tratamento das não conformidades seja aplicado na Organização conforme as melhores práticas de gestão de *compliance*.

É importante que o tratamento das não conformidades seja avaliado em relação à sua aplicabilidade e ao seu impacto antes da implementação na Organização. Caso o tratamento das não conformidades implique em alterações ou configurações na infraestrutura de TI, deve-se levar em conta as características do sistema em análise, visto que uma alteração de parâmetros de configuração ou de permissões no sistema de arquivos pode causar danos às aplicações.

4. CONTEXTO

O contexto da análise é a parte da gestão de *compliance* que envolve aspectos internos e externos da Organização. No **Módulo Risk Manager**, o contexto é representado fundamentalmente pelos requisitos selecionados, pelos objetos da análise e pela equipe envolvida. Alguns requisitos e objetos selecionados para a análise podem trazer outros elementos que passam a fazer parte do contexto, tais como requisitos, escalas de respostas e pesquisas, que são úteis para consolidar ou filtrar resultados. O projeto em análise possui as seguintes características:

Nome:	Auditoria de Incidentes e Requisições - 1º semestre 2021	Código:	PRJC21003
Situação:	Aberto	Data de Criação:	06/08/2021 10:47
Autor:	Charles Ferreira Falcao	Início da Análise:	06/08/2021 10:48
Líder:	Rejane Goldstein Telichevesky	Data de Fechamento:	
Líder Substituto:	Ricardo Krause Kurylenko		

Caso o projeto esteja em andamento, com situação “Aberto” na data de emissão do relatório, os resultados apresentados poderão ser parciais. Outras informações sobre o contexto do projeto podem ser obtidas através de consultas de *compliance*.

4.1 Requisitos investigados

Para cada requisito dos documentos de referência considerados, são apresentadas a quantidade de perguntas e a distribuição das respostas de perguntas de compliance conforme as escalas de resposta utilizadas. Seguem algumas observações importantes:

- O *Compliance Index* e o Nível de *Compliance* são calculados para as perguntas de *compliance* considerando as escalas de resposta selecionadas e as respostas escolhidas pelos entrevistados e são consolidados por requisito, documento de referência e objeto. Para informações adicionais sobre como o *Compliance Index* e o Nível de *Compliance* são calculados e consolidados, consulte o Manual do Usuário.
- Uma pergunta pode estar relacionada a mais de um requisito, de modo que o número de perguntas não necessariamente será igual ao número de requisitos.
- Podem existir requisitos sem perguntas diretamente relacionadas, incluídos apenas para agrupar outros requisitos de níveis inferiores.

Para cada documento de referência incluído no projeto, serão mostrados em uma tabela separada os requisitos analisados.

4.1.17 Processo de Gerenciamento de Incidentes

Requisitos	Qtd Perg	AT	PA	NA	Compliance Index	Nível de Compliance	Nível de Compliance Index
Relatar incidente / Solicitar serviços	0	0	0	0		Não Analisado	
Registrar incidente como resolvido e avaliar nova entrada na base de conhecimento	1	0	1	0	50,00%	Parcialmente Atendido	Média
Encaminhar para outra equipe	0	0	0	0		Não Analisado	
Contatar o usuário para fechar o chamado	1	0	1	0	50,00%	Parcialmente Atendido	Média
Reabrir o chamado	0	0	0	0		Não Analisado	
Enviar e-mail para o usuário	0	0	0	0		Não Analisado	
Fechar chamado	0	0	0	0		Não Analisado	
Iniciar atendimento pela área e investigar solução	1	0	1	0	50,00%	Parcialmente Atendido	Média
Abrir chamado vinculado (requisição, problema ou mudança)	0	0	0	0		Não Analisado	
Atribuir chamado ao fornecedor	1	1	0	0	100,00%	Atendido	Muito Alta
Registrar RESOLVIDO e avaliar nova entrada na base de conhecimento	1	0	1	0	50,00%	Parcialmente Atendido	Média
Tomar ciência	1	1	0	0	100,00%	Atendido	Muito Alta
Encaminhar chamado para a Central de Atendimento	0	0	0	0		Não Analisado	
Escalonar para o próximo nível	0	0	0	0		Não Analisado	
Categorizar chamado e Classificar como "Serviço Não Catalogad	1	1	0	0	100,00%	Atendido	Muito Alta
Verificar base de conhecimento	0	0	0	0		Não Analisado	
Verificar solução	0	0	0	0		Não Analisado	
Aplicar solução	0	0	0	0		Não Analisado	
Registrar incidente como resolvido e avaliar necessidade de requisição vinculada	1	0	1	0	50,00%	Parcialmente Atendido	Média
Abrir requisição vinculada	0	0	0	0		Não Analisado	
Encaminhar para equipe responsável	0	0	0	0		Não Analisado	

Total	8	3	5	0	68,75%	Parcialmente Atendido	Alta

Tabela 6.1 – Requisitos investigados

4.2 Plano da análise

O plano da análise foi definido durante o processo de planejamento do projeto e representa o escopo de objetos que se deseja analisar, os documentos de referência selecionados, seus requisitos e as pesquisas utilizadas. Os seguintes elementos foram considerados no plano:

4.2.1 Objetos que participaram da análise - 1

Ativo - 1

4.2.2 Documentos de referência - 1

Processo de Gerenciamento de Incidentes

4.2.3 Pesquisas - 1

Pesquisa do Processo de Gerenciamento de Incidentes e Requisições (5)- 1

Total de Perguntas - 5

Total de Entrevistados - 1

4.3 Gestão do projeto

Abaixo, a Tabela 7 mostra o líder e o líder substituto do projeto:

Nível	Função	Responsabilidades	Responsáveis
Gestão	Líder do projeto	Definir o escopo da análise Definir os analistas Monitorar a execução da análise Realizar consultas e gerar relatórios	**Rejane Goldstein Telichevesky**
Gestão	Líder substituto	Substituir o líder do projeto quando necessário.	**Ricardo Krause Kurylenko**

Tabela 7 – Equipe envolvida na análise

5. ANÁLISE CONSOLIDADA

As tabelas seguintes mostram os resultados da análise consolidados por documento de referência, requisito de primeiro nível e requisito de segundo nível. Seguem algumas observações importantes:

- O *Compliance Index* e o Nível de *Compliance* são calculados para as perguntas de *compliance* considerando as escalas de resposta selecionadas e as respostas escolhidas pelos entrevistados, e são consolidados por requisito, documento de referência e objeto. Para informações adicionais sobre como o *Compliance Index* e o Nível de *Compliance* são calculados e consolidados, consulte o Manual do Usuário.
- Uma pergunta pode estar relacionada a mais de um requisito, de modo que o número de perguntas não necessariamente será igual ao número de requisitos.
- Podem existir requisitos sem perguntas diretamente relacionadas, incluídos apenas para agrupar outros requisitos de níveis inferiores.

5.0 Processo de Gerenciamento de Incidentes

Documentos de referência	No. Req	AT	PA	NA	Compliance Index	Nível de Compliance	Nível de Compliance Index
Processo de Gerenciamento de Incidentes	8	3	5	0	68,75%	Parcialmente Atendido	Alta

Tabela 8 - Requisitos investigados

Requisitos de primeiro nível	Qtd Perg	AT	PA	NA	Compliance Index	Nível de Compliance	Nível de Compliance Index
Relatar incidente / Solicitar serviços	0	0	0	0		Não Analisado	
Registrar incidente como resolvido e avaliar nova entrada na base de conhecimento	1	0	1	0	50,00%	Parcialmente Atendido	Média
Encaminhar para outra equipe	0	0	0	0		Não Analisado	
Contatar o usuário para fechar o chamado	1	0	1	0	50,00%	Parcialmente Atendido	Média
Reabrir o chamado	0	0	0	0		Não Analisado	
Enviar e-mail para o usuário	0	0	0	0		Não Analisado	
Fechar chamado	0	0	0	0		Não Analisado	
Iniciar atendimento pela área e investigar solução	1	0	1	0	50,00%	Parcialmente Atendido	Média
Abrir chamado vinculado (requisição, problema ou mudança)	0	0	0	0		Não Analisado	
Atribuir chamado ao fornecedor	1	1	0	0	100,00%	Atendido	Muito Alta
Registrar RESOLVIDO e avaliar nova entrada na base de conhecimento	1	0	1	0	50,00%	Parcialmente Atendido	Média
Tomar ciência	1	1	0	0	100,00%	Atendido	Muito Alta
Encaminhar chamado para a Central de Atendimento	0	0	0	0		Não Analisado	
Escalonar para o próximo nível	0	0	0	0		Não Analisado	
Categorizar chamado e Classificar como "Serviço Não Catalogado"	1	1	0	0	100,00%	Atendido	Muito Alta
Verificar base de conhecimento	0	0	0	0		Não Analisado	
Verificar solução	0	0	0	0		Não Analisado	
Aplicar solução	0	0	0	0		Não Analisado	
Registrar incidente como resolvido e avaliar necessidade de requisição vinculada	1	0	1	0	50,00%	Parcialmente Atendido	Média
Abrir requisição vinculada	0	0	0	0		Não Analisado	
Encaminhar para equipe responsável	0	0	0	0		Não Analisado	
Total	8	3	5	0	68,75%	Parcialmente Atendido	Alta

Tabela 9 - Requisitos de primeiro nível

6. RECOMENDAÇÕES

No **Módulo Risk Manager**, as fases de avaliação e tratamento estão integradas com a fase de análise, como representado na Figura 5. As métricas obtidas na análise (*Compliance Index* e Nível de *Compliance*) devem ser consideradas na avaliação das não conformidades encontradas. Quando uma não conformidade é considerada inaceitável e você desejar tratá-la, é automaticamente gerado um evento para o seu tratamento, o qual pode ser monitorado no módulo *Workflow*.

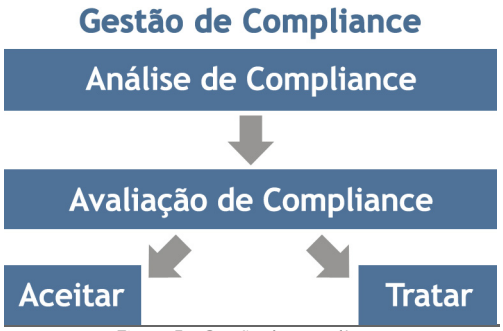

Figura 5 - Gestão de *compliance*

Para os próximos passos (avaliação e tratamento), sugerimos adotar a seguinte abordagem:

1) Identificar as não conformidades mais graves, observando quais requisitos possuem Nível de *Compliance* “Não Atendido”.

2) Considerar também a possibilidade de tratamento dos requisitos com Nível de *Compliance* “Parcialmente Atendido”.

3) Enviar para tratamento as não conformidades identificadas nos passos anteriores, levando em consideração a sua gravidade e os impactos do tratamento.

4) Justificar a aceitação das não conformidades que não forem enviadas para tratamento.

5) Monitorar, através do módulo *Workflow*, os eventos de tratamento gerados para o projeto.