

TOP PRACTICES

ANÁLISE DE MATURIDADE DE PROCESSOS DE OPERAÇÃO E MANUTENÇÃO DE DATA CENTER - FOMM

1. INTRODUÇÃO

Uma das principais causas de *downtime* em *Data Centers* são os erros humanos. Os erros humanos podem ser de caráter intencional (ex: vandalismo e sabotagem) ou não intencional, que ocorrem por deficiência técnica ou falha na aplicação de processos e execução de procedimentos.

Este trabalho de avaliação da estrutura de operação e manutenção e dos processos e procedimentos existentes visa identificar possíveis exposições a riscos de erros humanos que poderiam levar a um *downtime* e servirão como base para um trabalho futuro de assessoria para levar a área de operação e manutenção a um padrão de classe mundial e eventual obtenção de certificação.

O foco das equipes de Operação e Manutenção está na prevenção de falhas e defeitos, na confiabilidade, performance e na plena disponibilidade dos ativos do Data Center e salas técnicas que suportam os ambientes de TI.

2. METODOLOGIA E EXPERIÊNCIA

A metodologia de trabalho alia técnicas de Gerência de Projeto, Metodologias Ágeis e conformidade com as normas ISO/IEC 19011: 2018 (Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental) e ISO IEC 17021-1: 2016 (Avaliação da conformidade - Requisitos para organismos que fornecem auditoria e certificação de sistemas de gestão), à nossa experiência contínua de 9 anos na auditoria de métodos e procedimentos de operação e manutenção de facilities de Data Centers de todos os portes e segmentos de mercado:

- A) Controle do processo: **PMI – PMP Gerenciamento de Projetos (Guia PMBOK®)** seus elementos de processos do gerenciamento de projetos que são:
- Início
 - Planejamento
 - Execução
 - Monitoramento e Controle
 - Encerramento
- B) Métodos Ágeis para gerar um ambiente colaborativo entre as partes envolvidas, gerando sinergia e aproveitando oportunidades de recursos disponíveis para garantir entregas mais assertivas e mensuráveis:
- Comunicação
 - Praticidade
 - Alinhamento de Expectativas
 - Colaboração
 - Adaptabilidade
 - Flexibilidade

C) Auditores Certificados em Ambientes Críticos – **CEA ICOR** – Processo de Método de Levantamento, Análise de *Gaps* e *Findings*.

Ordem da Auditoria:

- Priorizar – Priorizar a ordem de importância e probabilidade de ocorrência de *outage*
- Engajar – Pessoas do ambiente a ser auditado
- Realizar – Execução das etapas de auditoria para coletar os dados
- Avaliar – Avaliação dos resultados
- Revisar – Comentar os resultados e apontar recomendações

3. FRAMEWORK

O Framework base aplicado na avaliação é o FOMM - Facility Operations Maturity Model. O FOMM é um modelo de referência de mercado que não se baseia em tecnologias ou produtos, mas apenas relaciona os processos e elementos de Operação e Manutenção de Facilities comuns de mercado. Ele se destina a servir como um instrumento de referência (*benchmarking tool*) para ajudar na avaliação de diferentes categorias e disciplinas, bem como auxiliar na comparação com outras instalações similares.

O FOMM foi desenvolvido como uma abordagem padronizada para avaliar e qualificar o método pelo qual os Data Centers são operados, com base na realidade da observação das operações de instalações críticas de um grande número de clientes em mais de 30 anos. Ele fornece uma orientação para organizações e terceiros envolvidos nas operações de instalações críticas que desejam desenvolver mais o modelo de operação de sua infraestrutura crítica.

Com esse modelo é possível aferir os atuais níveis de maturidade para permitir que as organizações priorizem metas para obter níveis mais elevados de maturidade, alinhados com os objetivos de negócios, bem como a criação de uma estratégia para alcançá-los.

O modelo está dividido em sete (7) disciplinas que são divididas em elementos e subelementos.

3.1 Disciplinas e Elementos do FOMM



7 Disciplinas
25 Elementos
78 Subelementos

Fig 1. FOMM Facility Operations Maturity Model

I. Segurança e Saúde / Ambiental (SSMA)

Programas de *facilities* com foco em conformidade com aspectos regulatórios de saúde, segurança e meio ambiente.

- Programa de segurança no trabalho;
- Equipamento de Proteção Individual (EPI);
- Segurança elétrica;
- Análise de riscos;
- Comunicação de riscos;
- Materiais perigosos;
- Conformidade legal (Ambiental, Saúde, Incêndio, etc.).

II. Preparação e Resposta para Emergência

Estes são os processos estabelecidos para antecipar, prevenir e mitigar os efeitos de incidentes emergentes e situações de emergência.

- EOP - Procedimentos Operacionais de Emergência;
- Plano de Gestão de Crises;
- Procedimentos de Continuidade de Negócios / Recuperação de Desastres (BC/DR);
- Processo de Simulações, Procedimentos, Programação e Execução;
- Gerenciamento de Incidentes (Notificação, Identificação de Incidente e Reporte, "Lições Aprendidas" / Relatórios de "Quase Falhas").

III. Gestão de Manutenção

Tarefas associadas à conservação, manutenção e reparação dos sistemas de infraestrutura física de apoio aos objetivos de desempenho de *facilities*, confiabilidade e nível de serviço.

- Gestão de Ativos (Banco de Dados de Ativos e Escopo de Serviços);
- Gestão de Ordem de Serviços (Agendamento e Acompanhamento; Registro e Análise; Corretiva ou Seguimento (*Follow-on*) das atividades; Relatórios);
- CMMS (Computerized Maintenance Management System - Administração; Utilização e Funcionalidades);
- Gestão de Vendors (Terceiros) (Seleção; Métricas de Performance e Relatórios de Serviços);
- Gestão de Peças Sobressalentes (Identificação, Inventário e Estoque).

IV. Gestão do Site

Atividades do dia a dia, associadas com a utilização do site, desempenho e eficiência.

- Gestão de Infraestrutura (Monitoramento de *Facilities*; Gestão de Capacidade e Relatórios; DCIM);
- Operação do Site (Processos Administrativos e Procedimentos; Documentação Técnica; Regras de Trabalho em *Critical Facilities*; Mudanças de Turnos; Rondas no Edifício);

- Eficiência e Otimização (Avaliação de Desempenho; Gestão de Energia e Relatórios; Otimização de Sistemas);
- Condições do Site (Limpeza e Organização; Materiais e Inventário).

V. Gestão de Operações

Atividades do dia a dia, de suporte à operação segura, transparente e *cross-functional* do Data Center.

- Gestão de Pessoal (Modelagem de Equipe e Utilização; Desenvolvimento de Carreira);
- Medição de desempenho (SLA – *Service Level Agreement*; Principais indicadores de desempenho);
- Gestão de Riscos (Identificação e Comunicação de Risco do Site; Controle de acesso; Orientação de *Vendors* e Visitantes; Cumprimento de protocolo de segurança do site);
- Gestão Financeira (Compras, faturamento e contenção de custos);
- Relatórios (Relatórios de Gestão de Operações).

VI. Gestão de Mudanças

Os métodos, técnicas e ferramentas destinadas a assegurar a coordenação e execução dos trabalhos planejados de forma segura e bem-sucedida, realizados no prazo e com a mínima interrupção dos serviços.

- Análise de Riscos e Comunicação (Identificação de riscos e documentação; Notificação e Operações);
- Desenvolvimento e Revisão de Procedimento Operacional (SOP e MOP);
- Práticas de Controle de Mudanças (Práticas de trabalho estruturado; Supervisão de *Vendors*).

VII. Gestão de Qualidade

A conquista da excelência operacional através do uso de Garantia de Qualidade (*Quality Assurance*), Controle de Qualidade (*Quality Control*) e medidas de Melhoria da Qualidade (*Quality Improvement*) na prevenção, detecção e correção de erros.

- Gestão de Documentos (Sistema de Gestão de Documentos; Controle de Versões)
- Treinamento (Análise de Necessidades; Qualificação/Licenciamento/Certificação; Registros; Lições Aprendidas)
- Inspeções de Auditorias (Checagem de Qualidade pelos operadores do site; Programa de auditoria periódica por QC);
- Melhoria Contínua (Análise de Falhas; RCA – Análise de Causa Raiz; Programa de Inovações).

3.2 Maturity Scores

Cada subelemento é definido por cinco (5) níveis de maturidade. Estes níveis são baseados na estrutura do modelo de maturidade do IT Governance Institute (COBIT), graduados ou classificados numa escala de "1" a "5", sendo de "1" menos maduro a "5" para o mais desenvolvido, conforme abaixo:

Níveis de Maturidade de Operação de Facilities



Fig 2a. Maturity Score

- 0 - Inexistente** - Completa falta de quaisquer processos reconhecíveis.
- 1 - Inicial / Ad Hoc** - Existem processos, no entanto, não padronizado.
- 2 - Repetível, mas intuitivo** - Comportamento repetido, porém sem um procedimento formal.
- 3 - Processos definidos** - Procedimentos foram padronizados e documentados, mas não sofisticados.
- 4 - Gerenciado e Mensurável** - Processos estão sob constante melhoria e fornecem boas práticas.
- 5 - Otimizado** – Processos refinados em melhores práticas e com base nos resultados de melhoria contínua e modelagem de maturidade de mercado.

Este uso prático de pontuação permite visibilidade da maturidade pelos administradores e membros do comitê de auditoria e ao mesmo tempo, fornece às entidades auditadas uma visão clara de como o seu perfil de controle se parece, cria um ambiente propício para discussão e uma referência para medição da evolução de maturidade dos processos.

Nonexistent	Initial/Ad hoc	Repeatable but intuitive	Defined	Managed and Measurable	Optimized
0	1	2	3	4	5
To solve ASAP	To solve	To improve	Acceptable	Good	Excellent

Fig 2b. Maturity Score

4. Exemplo de análise de subelemento no Relatório FOMM:

Para o subelemento abaixo, o Cliente definiu em 2017 o nível de maturidade 3 como objetivo e foram coletadas evidências em 2017 e em 2020 (após trabalho evolutivo).

II.1 EOP - Procedimentos Operacionais de Emergência

Nível	Descrição	Observação
5	<ul style="list-style-type: none"> Os EOPs são examinados através de análises críticas de incidentes ou de algum processo de revisão periódica. 	
4	<ul style="list-style-type: none"> A Gerência monitora regularmente o uso de EOPs e toma as medidas apropriadas. Os membros da equipe operacional responsáveis pela execução desses procedimentos recebem treinamento documentado e avaliação periódica de sua compreensão. Os procedimentos são publicados e estão prontamente disponíveis na área de uso. 	
3	<ul style="list-style-type: none"> Procedimentos operacionais de emergência (EOPs) padronizados estão desenvolvidos e disponíveis para cenários de emergência prováveis e/ou consequentes. Treinamento foi fornecido a todo o pessoal. Os EOPs não são utilizados consistentemente durante situações de emergência. 	<p>3.1</p> <p>3.2 / 3.3</p> <p>3.4 / 3.5 / 3.6</p>
2	<ul style="list-style-type: none"> Capacidade de resposta a emergências foi desenvolvida e demonstrada, porém não é utilizada documentação padronizada de procedimentos operacionais de emergência (EOPs). Pode haver documentação para falhas ou incidentes repetidos. 	X
1	<ul style="list-style-type: none"> Existem poucos ou nenhum procedimento coordenado de Resposta de Emergência (ações). 	X
0	<ul style="list-style-type: none"> Inexistente 	X

Inexistente 0	Inicial / Ad Hoc 1	Repetível, mas intuitivo 2	Definido 3	Gerenciado e Mensurável 4	Otimizado 5
	●		● ↑		
Para resolver ASAP	Para resolver	Para melhorar	Aceitável	Bom	Excelente

● ⇒ Situação Atual

● ⇒ Situação 2017

↑ ⇒ Objetivo

EVIDÊNCIAS / DOCUMENTOS RECEBIDOS:

Entrevistas com a equipe de Operação DC onde buscavam as respostas e apresentação de evidências.

Documentos:

ADM-000x - LISTA DE EQUIPAMENTOS CRITICOS
ADM-000x - CENÁRIOS DE FALHAS
ADM-000x - PLANO DE COMUNICAÇÃO FACILITIES

Apresentados também os EOPs já elaborados e listados no documento de Cenários de Falhas.

ANÁLISE:

3.1 Existem já alguns procedimentos de emergência (EOPs) elaborados e padronizados, porém ainda em andamento os trabalhos, conforme documento de Cenários de Falhas.

Os EOPs estão arquivados na biblioteca de Missão Crítica e também fisicamente, assim como também os documentos de Cenário de Falhas, Lista de Equipamentos Críticos e Plano de Comunicação.

Não existe ainda uma uniformidade da equipe com relação a conhecer a localização de todos os documentos.

3.2 Foram realizados treinamentos de mecânica (2020) e elétrica (2019), porém os de elétrica ainda não foram reciclados em 2020, mas serão realizados, conforme cronograma desenvolvido durante a auditoria.

3.3 Exercícios *tabletop** não estão sendo realizados para estimular a participação de todos os envolvidos e a melhoria contínua dos procedimentos.

3.4 Não encontrado evidência de utilização de EOPs; a informação passada foi que usaram o conhecimento contido neles, mas não com o documento em mãos, porém pelo staff e não pelo operador, que deveria fazer a primeira intervenção ao invés de aguardar o staff chegar. Foi relatado que há um checklist que também é utilizado, mas que também não foi aplicado e considerado, pois não foi apresentada evidência.

3.5 Em relatórios de incidentes apresentados, foi verificado que o 2º nível tem comportamento de missão crítica mais desenvolvido e mais clareza na solução do problema do que o 1º nível, em relação a processos e procedimentos, mas ao menos demonstraram saber utilizar o plano de comunicação corretamente.

3.6 Foi elaborado um EOP-1xxx de falha de energia após o incidente INCyyy para que a Operação possa seguir, porém apesar de Missão Crítica ser 24x7, a engenharia não é. Foi comentado pela engenharia, que em uma emergência fora do horário comercial existirá um tempo de deslocamento entre 1,5 e 2 horas e que o diesel do gerador tem autonomia de 4 horas.

RECOMENDAÇÕES:

Dar continuidade no desenvolvimento dos outros procedimentos operacionais de emergência (EOPs).

Além de cenários de falhas de equipamentos, devem ser desenvolvidos EOPs para eventos externos como, por exemplo, situações climáticas extremas, interrupções de serviços de concessionárias, desabastecimento de combustível, greves e manifestações.

Desenvolver treinamentos práticos rotineiros, com avaliação.

Promover exercícios *tabletop**.

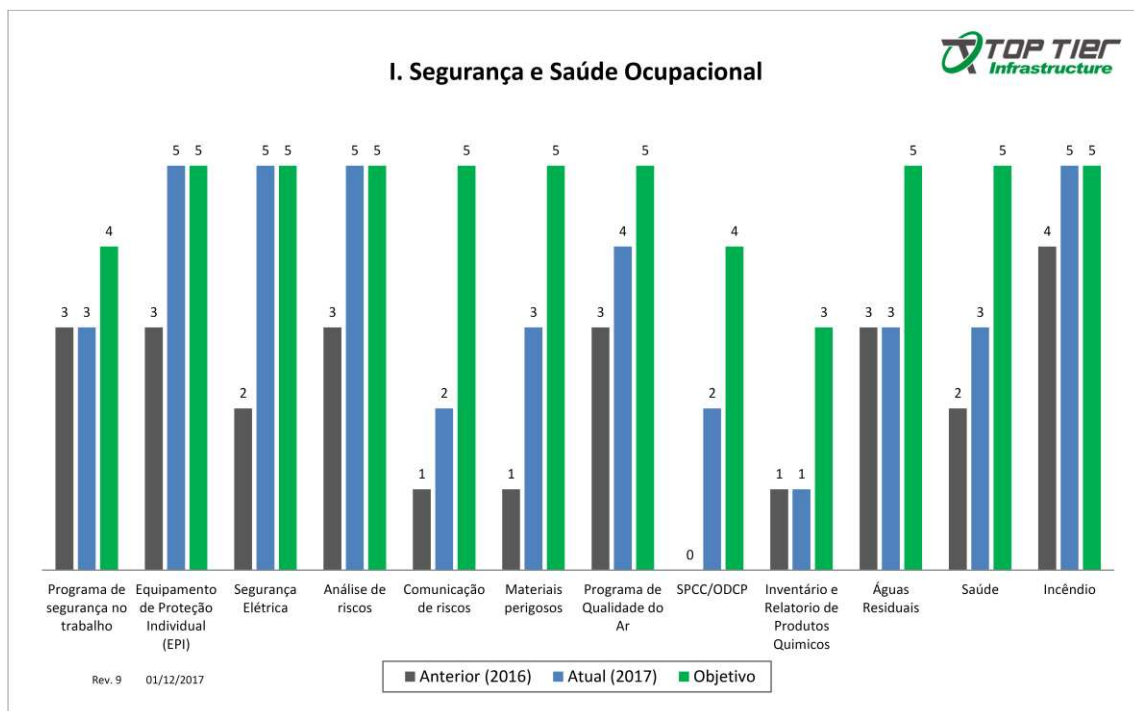
Os EOPs devem ser considerados parte da Biblioteca de Documentos Críticos dos sites e sua gestão deve estar em linha com política específica e também arquivados fora do site, de modo que eles possam ser facilmente acessados em caso de emergência.

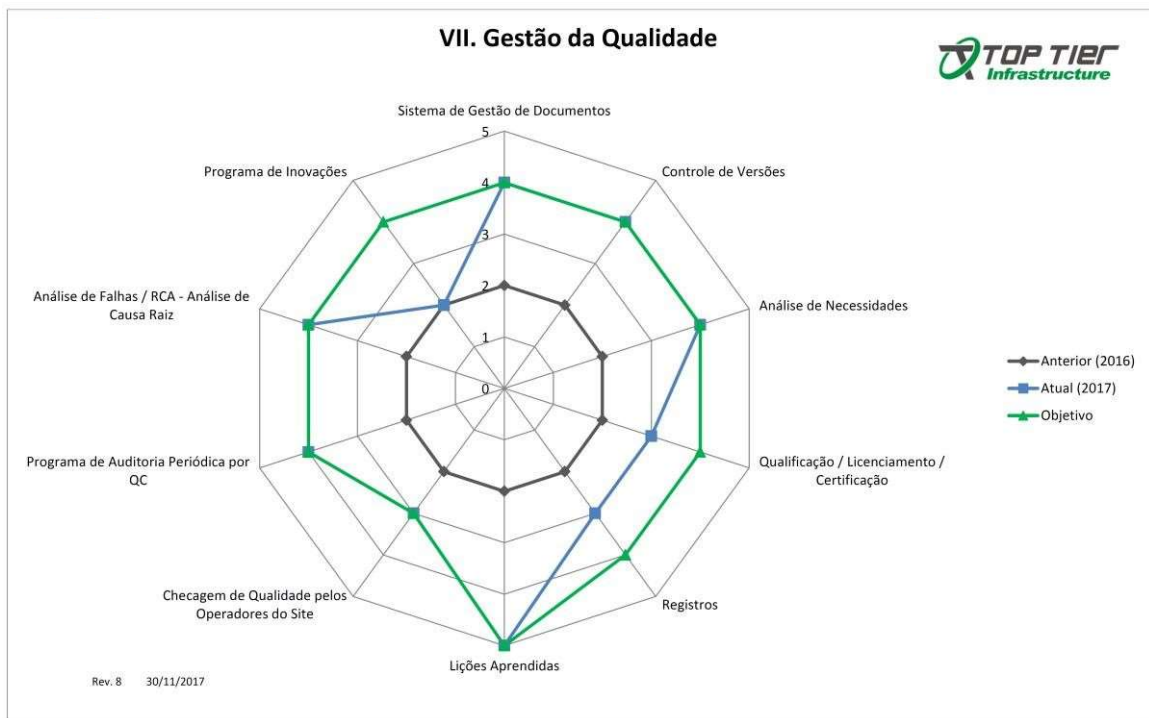
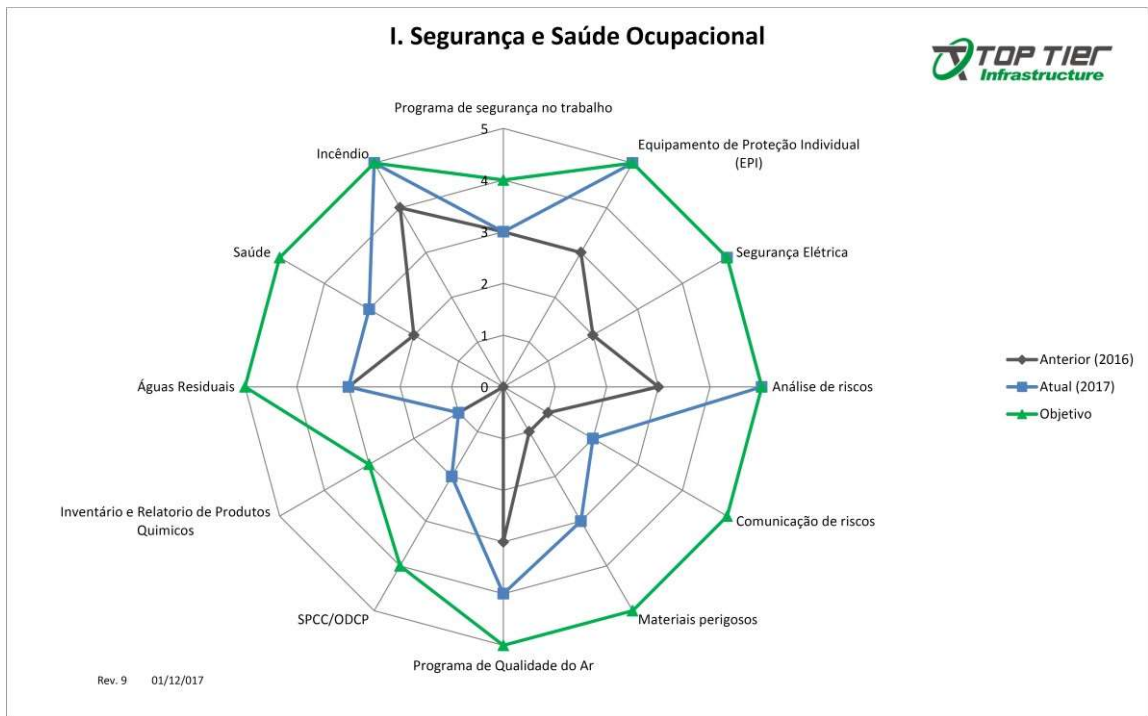
O Cliente deve avaliar os itens abaixo para operar com segurança 7x24:

- 1- Ter alguém da engenharia no local fora do horário comercial;
- 2- Capacitar alguém da Operação DC para operar o GMG;
- 3- Ter um GMG backup
- 4- Ter um contrato de reposição de diesel 7x24
- 5- Uma combinação das anteriores.

* Um exercício *tabletop* envolve pessoal chave discutindo cenários simulados em um ambiente informal e podem ser utilizados para avaliar planos, políticas e procedimentos. Pode incluir a participação de especialistas externos e fabricantes/fornecedores.

5. Exemplos de apresentação executiva dos resultados do Relatório FOMM para gestão da evolução da maturidade de operação:

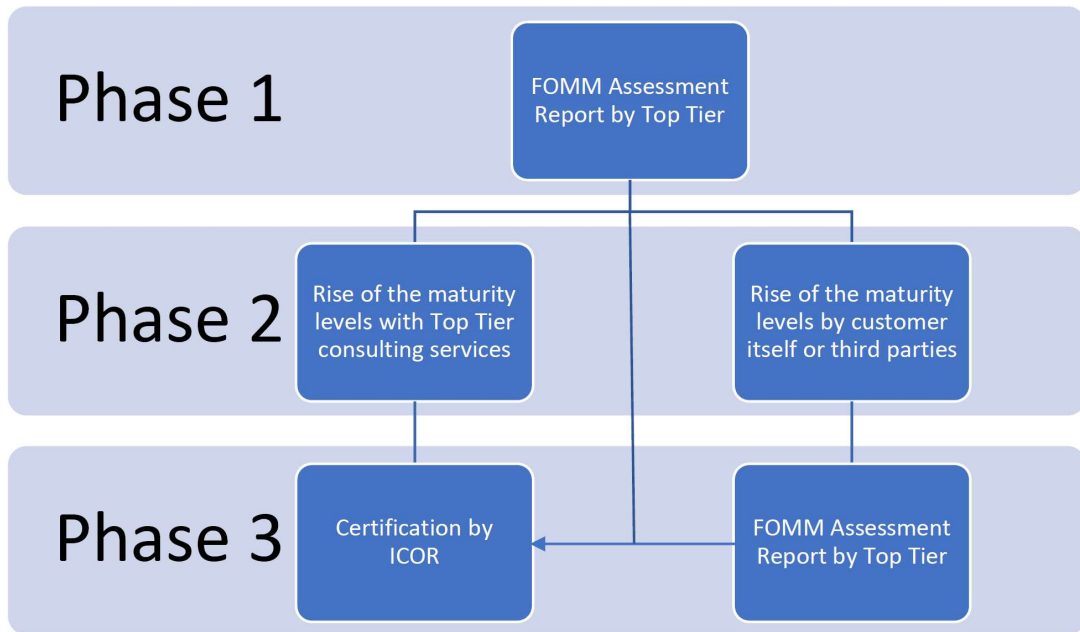




6. **Certificação FOMM acreditada pelo ICOR**
<https://www.build-resilience.org/>



PATHS TO FOMM CERTIFICATION



VALIDADE: 3 ANOS

REVISÃO DE SCORE: ANUAL (ISO/IEC 17021-1:2016) 