EDM01 - Assegurar a Governança de TI (Estratégia e Direção da Governança de TI) é um dos objetivos do framework COBIT (Control Objectives for Information and Related Technologies), que é um modelo reconhecido internacionalmente para governança e gestão de TI em organizações.

O objetivo do EDM01 é garantir que uma estrutura de governança de TI eficaz esteja estabelecida e mantida na organização. A governança de TI refere-se ao conjunto de processos, políticas, diretrizes e estruturas que garantem que a TI esteja alinhada aos objetivos estratégicos da organização, além de fornecer supervisão e controle adequados sobre os recursos de TI.

Para atingir esse objetivo, algumas atividades-chave devem ser realizadas:

- Avaliação das estruturas de governança existentes: A organização deve realizar uma avaliação para determinar a adequação das estruturas de governança de TI existentes. Isso envolve a análise dos processos de tomada de decisão, as responsabilidades e as estruturas de prestação de contas relacionadas à TI. A ideia é identificar lacunas e áreas de melhoria.
- Orientação para melhorias: Com base na avaliação das estruturas de governança de TI, devem ser fornecidas orientações para melhorias. Isso pode incluir recomendações para a criação de comitês ou grupos de governança de TI, a definição de papéis e responsabilidades claros, o estabelecimento de políticas e diretrizes, entre outras medidas.
- Comunicação e aplicação de políticas e diretrizes: É fundamental que as políticas e diretrizes de governança de TI sejam comunicadas em toda a organização e aplicadas de maneira consistente. Isso ajuda a garantir que todos os funcionários compreendam as expectativas e os requisitos de governança de TI e ajuda a criar uma cultura de responsabilidade e conformidade.

Em resumo, o EDM01 visa estabelecer uma estrutura de governança de TI eficaz dentro da organização. Isso envolve avaliar as estruturas existentes, fornece orientações para melhorias, comunicar e aplicar políticas e diretrizes de governança de TI. Ao fazer isso, a organização pode garantir que a TI esteja alinhada com os objetivos estratégicos e que os recursos de TI sejam supervisionados e controlados de maneira adequada. Isso é fundamental para garantir a eficácia e o valor agregado da TI na organização.

Exemplo de processo e política para expressar o funcionamento do objetivo EDM01 - Assegurar a Governança de TI:

Processo: Avaliação e Melhoria da Governança de TI

1. Objetivo: O objetivo deste processo é avaliar continuamente as estruturas de governança de TI existentes e fornecer orientações para melhorias, a fim de garantir uma governança de TI eficaz na organização.

2. Atividades do processo:
   2.1. Avaliação da governança de TI:
   - Realizar uma análise detalhada das estruturas de governança de TI existentes, incluindo processos de tomada de decisão, responsabilidades e estruturas de prestação de contas relacionadas à TI.

- Identificar lacunas e áreas de melhoria na governança de TI por meio de revisões e avaliações regulares.

2.2. Recomendações de melhoria:

- Com base na avaliação da governança de TI, fornece orientações e recomendações claras para melhorias.
- Identificar e priorizar as ações necessárias para fortalecer a governança de TI.

2.3. Implementação de melhorias:

- Desenvolver planos de ação para implementar as melhorias recomendadas.
- Designar responsáveis por cada ação e estabelecer prazos para sua conclusão.
- Monitorar o progresso das iniciativas de melhoria e realizar ajustes conforme necessário.

3. Política: Governança de TI

3.1. Objetivo:

- Estabelecer uma estrutura de governança de TI eficaz que garanta a conformidade com os objetivos estratégicos da organização, bem como a supervisão e controle adequados sobre os recursos de TI.

3.2. Diretrizes:

- As estruturas de governança de TI devem ser revisadas regularmente para garantir sua adequação contínua.
- Devem ser estabelecidos papéis e responsabilidades claros para as partes envolvidas na governança de TI.
- Deve haver comunicação efetiva de políticas e diretrizes de governança de TI em toda a organização.
- As políticas de governança de TI devem ser aplicadas de forma consistente e as violações devem ser tratadas de acordo com os procedimentos estabelecidos.
- Deve ser promovida uma cultura de responsabilidade e conformidade em relação à governança de TI.

3.3. Responsabilidades:

- A equipe de governança de TI é responsável por conduzir a avaliação contínua da governança de TI e fornece recomendações de melhoria.
- A alta direção é responsável por garantir que as políticas de governança de TI sejam estabelecidas, comunicadas e aplicadas em toda a organização.
- Todos os funcionários devem cumprir as políticas e diretrizes de governança de TI e relatar quaisquer violações ou preocupações às partes apropriadas.

O objetivo EDM03 (Assegurar a Gestão de Riscos de TI) está relacionado à implementação eficaz e alinhada com os objetivos de negócios da gestão de riscos de Tecnologia da Informação (TI). A gestão de riscos de TI é um processo essencial para garantir a segurança e o bom funcionamento dos sistemas de informação de uma organização.

A gestão de riscos de TI envolve várias etapas, incluindo a identificação, avaliação, resposta, monitoramento e comunicação dos riscos. Vamos explorar cada uma dessas etapas em detalhes:

1. Identificação de riscos: O primeiro passo é identificar os riscos potenciais que podem afetar a segurança e a disponibilidade dos sistemas de informação. Isso pode ser feito por meio de análises de vulnerabilidades, revisões de processos, inspeções de infraestrutura e outras técnicas. A identificação de riscos deve abranger tanto os riscos

internos (como falhas de segurança, problemas de infraestrutura) quanto os riscos externos (como ataques cibernéticos, desastres naturais).

2. Avaliação de riscos: Uma vez que os riscos são identificados, é necessário avaliar sua probabilidade de ocorrência e impacto potencial. A avaliação de riscos permite priorizar os riscos com base em sua gravidade e definir ações adequadas para lidar com eles. Essa avaliação pode ser feita utilizando técnicas como a análise quantitativa (atribuindo valores numéricos para probabilidade e impacto) ou análise qualitativa (classificando os riscos em categorias de baixo, médio ou alto).
3. Resposta aos riscos: Após a avaliação dos riscos, é importante desenvolver e implementar estratégias de resposta adequadas para lidar com cada risco identificado. As estratégias de resposta podem variar de acordo com a natureza do risco e incluem opções como mitigação (reduzir a probabilidade ou impacto do risco), transferência (transferir o risco para terceiros, como um seguro), aceitação (aceitar o risco sem ação adicional) ou evitação (evitar completamente o risco).
4. Monitoramento contínuo: A gestão de riscos de TI é um processo contínuo que requer monitoramento constante dos riscos identificados. Isso envolve a implementação de controles de segurança adequados, auditorias regulares, análise de incidentes e revisões periódicas dos riscos. O monitoramento contínuo permite identificar mudanças nas condições de risco e ajustar as estratégias de resposta conforme necessário.
5. Comunicação de informações sobre riscos: É fundamental comunicar adequadamente as informações sobre riscos para as partes interessadas relevantes, incluindo a alta administração, os proprietários de processos de negócios e as equipes de TI. A comunicação eficaz sobre os riscos permite que as partes interessadas entendam os riscos associados à infraestrutura de TI e tomem decisões informadas para mitigar esses riscos. Isso pode envolver relatórios periódicos, painéis de controle de risco, workshops de conscientização e outras formas de comunicação que sejam adequadas e compreensíveis para as partes interessadas.

Além dessas etapas específicas, é importante ressaltar que a gestão de riscos de TI deve ser integrada às atividades de governança corporativa e aos processos de gerenciamento de riscos mais amplos da organização. Isso significa que a gestão de riscos de TI deve estar alinhada com a estratégia de negócios e os objetivos organizacionais, e que os riscos de TI devem ser tratados como parte integrante dos riscos gerais da organização.

Para garantir a eficácia da gestão de riscos de TI, é recomendado seguir boas práticas e frameworks reconhecidos, como o COSO ERM (Enterprise Risk Management), o ISO/IEC 27005 (gestão de riscos de segurança da informação) e o NIST SP 800-30 (gestão de riscos de TI). Esses frameworks fornecem orientações detalhadas sobre como identificar, avaliar e responder aos riscos de TI de forma eficiente.

Além disso, é essencial que a gestão de riscos de TI seja apoiada por uma cultura organizacional que valorize a segurança da informação e a conscientização dos funcionários. A educação e treinamento dos colaboradores sobre os riscos de TI e as medidas de segurança adequadas são fundamentais para reduzir a probabilidade de ocorrência de incidentes e fortalecer a postura de segurança da organização.

Em resumo, o objetivo EDM03 visa garantir que a gestão de riscos de TI seja implementada de forma eficaz, abrangendo a identificação, avaliação, resposta, monitoramento e comunicação adequada dos riscos de TI. Isso contribui para proteger os ativos de informação

da organização, minimizar os impactos de incidentes de segurança e garantir a continuidade dos negócios.

um exemplo de um processo para a gestão de riscos de TI, que pode ser utilizado como base para a criação de uma política:

1. Objetivo: O objetivo deste processo é estabelecer uma abordagem estruturada e eficaz para identificar, avaliar, responder, monitorar e comunicar os riscos de TI, garantindo que a gestão de riscos esteja alinhada com os objetivos de negócios da organização.
2. Escopo: Este processo se aplica a todas as atividades de TI e sistemas de informação da organização, abrangendo todos os departamentos e funcionários envolvidos na gestão de riscos de TI.
3. Responsabilidades:

3.1. Diretoria Executiva:

- Definir a estratégia e a política de gestão de riscos de TI.

- Aprovar os recursos e o orçamento necessários para a implementação da gestão de riscos de TI.

- Monitorar e revisar periodicamente os resultados e o desempenho da gestão de riscos de TI.

3.2. Gerente de Riscos de TI:

- Coordenar e supervisionar a implementação do processo de gestão de riscos de TI.

- Facilitar a identificação e avaliação dos riscos de TI em todas as áreas da organização.

- Desenvolver e implementar estratégias de resposta aos riscos.

- Monitorar continuamente os riscos de TI e revisar as estratégias de resposta, conforme necessário.

- Comunicar os riscos de TI e os resultados do processo de gestão de riscos às partes interessadas relevantes.

3.3. Equipe de TI e demais departamentos:

- Identificar e relatar os riscos de TI relacionados às suas respectivas áreas de atuação.

- Participar da avaliação e definição de estratégias de resposta aos riscos.

- Implementar controles de segurança adequados para mitigar os riscos identificados.

- Monitorar e reportar regularmente os riscos e incidentes de segurança.

4. Etapas do processo:

4.1. Identificação de riscos:

- Realizar análises de vulnerabilidades, revisões de processos, inspeções de infraestrutura e outras técnicas para identificar os riscos de TI.

- Documentar os riscos identificados e atribuir uma classificação de probabilidade e impacto.

4.2. Avaliação de riscos:

- Realizar uma avaliação detalhada de cada risco identificado, considerando a probabilidade de ocorrência e o impacto potencial.

- Priorizar os riscos com base na sua gravidade e classificá-los em categorias de baixo, médio ou alto risco.

4.3. Resposta aos riscos:

- Desenvolver e implementar estratégias de resposta adequadas para cada risco identificado.

- As estratégias de resposta podem incluir medidas de mitigação, transferência, aceitação ou evitação de riscos.

4.4. Monitoramento contínuo (continuação):

- Realizar auditorias regulares para garantir a efetividade dos controles de segurança implementados.

- Monitorar continuamente os riscos identificados, avaliar mudanças nas condições de risco e ajustar as estratégias de resposta, conforme necessário.

- Registrar e analisar os incidentes de segurança e aprender com eles para melhorar as medidas de mitigação e prevenção.

4.5. Comunicação de informações sobre riscos:

- Estabelecer canais de comunicação adequados para transmitir informações sobre os riscos de TI às partes interessadas relevantes.

- Preparar relatórios periódicos de riscos, painéis de controle de risco e outras formas de comunicação que sejam compreensíveis e acionáveis.

- Realizar workshops de conscientização sobre riscos de TI para os funcionários, destacando as melhores práticas e medidas de segurança a serem adotadas.

5. Revisão e melhoria:

- Periodicamente, revisar e avaliar a eficácia do processo de gestão de riscos de TI.

- Realizar revisões de conformidade, auditorias internas e externas para identificar áreas de melhoria.

- Atualizar a política, os procedimentos e os controles de segurança, conforme necessário, com base nas lições aprendidas e nas mudanças do ambiente de riscos de TI.

Essa estrutura de processo pode ser adaptada e personalizada de acordo com as necessidades e requisitos específicos da organização. É importante envolver os principais stakeholders, incluindo a alta administração, a equipe de TI e os proprietários de processos de negócios, na definição, implementação e revisão do processo de gestão de riscos de TI.