Metodologia FRAAP

Facilitated **R**isk **A**nalysis and **A**ssessment **P**rocess

Equipa:

Diogo Amaral	93228
Guilherme Pereira	93134
José Costa	92996

FRAAP

O FRAAP é uma metodologia que tem como objetivo efetuar de forma mais rápida e eficaz uma análise de risco sobre sistemas ou processos.

Fases do FRAAP

Pre-FRAAP

Duração: 1 a 1,5 horas

Envolve: O gestor de negócio e o de projeto, o facilitador e o escriba

FRAAP

Duração: até 4 horas

Envolve: Todos os elementos da equipa

Post- FRAAP

Duração: 1 a 2 semanas

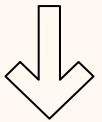
Realizado pela equipa de consultores

Pre-FRAAP

- O Pre-FRAAP é uma breve reunião inicial que serve de preparação para a reunião FRAAP.

- Esta reunião deve assim envolver o gestor de Negócios/processos e Gestor de Projeto assim como a equipa de consultores.

- É esperado que nesta reunião se obtenha os seguintes resultados.



Resultados do Pre-FRAAP

Pre-Triagem

Determinar que elementos necessitam ou não de uma avaliação de Risco

Definição do âmbito

Determinar qual é o âmbito da avaliação a realizar

Diagrama do sistema

Detalhe de um diagrama com a descrição do processo em análise

Serve para documentar e informar a equipa FRAAP

Estabelecimento da equipa

Identificar os elementos que vão estar envolvidos no processo

Resultados do Pre-FRAAP

Requisitos para a sessão FRAAP

Perceber o que é necessário para realizar a próxima reunião (data da reunião, local da reunião,...)

Mini-Brainstorming

No sentido de identificar algumas ameaças como introdução à reunião FRAAP

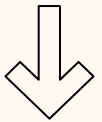
Acordar definições

Definir o significado de algumas definições que são usadas durante o processo

FRAAP

- Principal reunião que dura cerca de 4 horas e que envolve todos os elementos da equipa identificados anteriormente

- É esperado que nesta reunião se obtenha os seguintes resultados.



Resultados da sessão FRAAP

1 Identificar ameaças

2 Identificar controlos existentes

3 Calcular riscos

Resultados da sessão FRAAP

4 Identificar novos controlos

5 Caracterização de riscos residuais

Post-FRAAP

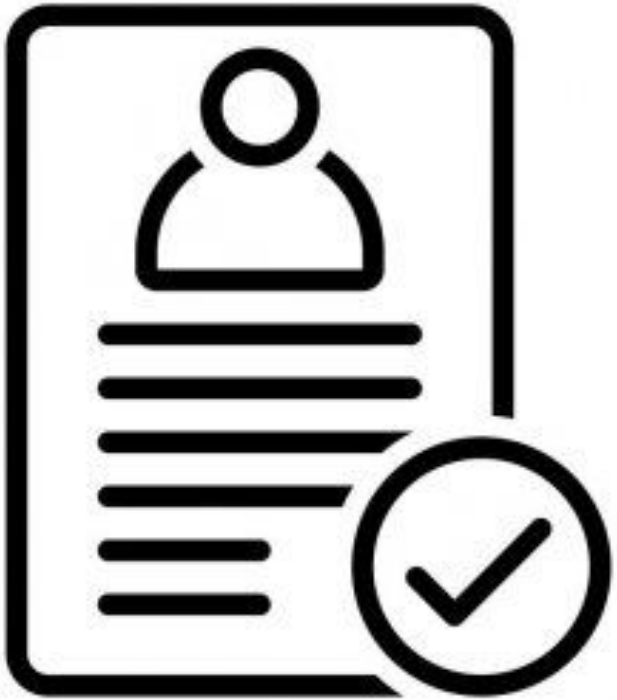
Relatório final

Contendo sumário executivo, resumo da reunião, identificação dos controlos e análise do processo

Apresentação das conclusões

Apresentação final das conclusões ao Gestor de Negócio

Discussão



Definições

1.Definições - termos técnicos

Tendo por base, as definições no **NIST**(National Institute of Standards and Technology), **ISO** 27001(International Organization for Standardization), **RGPD**(Regulamento Geral de Proteção de Dados) entre outros propomos as seguintes definições

Ameaça	Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização
Ativo	É um recurso com valor. Pode ser uma pessoa, um processo, informação,...
Dados Pessoais	Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular

Incidente	Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação
Violação de dados pessoais	Uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento
Impacto	O efeito de uma ameaça sobre um ativo, expresso em termos tangíveis ou intangíveis
Risco	Risco é uma combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados
Vulnerabilidade	É uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um ativo de informação
Probabilidade	Quantificação da possibilidade uma dada ameaça acontecer

Avaliação do risco

Para a avaliação de risco temos duas propostas

1. Usar a template de avaliação de risco fornecida pelo NIST
2. Template criada por esta equipa

1.Níveis de avaliação (probabilidade)

Nivel	Impacto	Descrição de impacto
1	Baixo	Não é provável que aconteça
2	Médio	Pode acontecer raras vezes
3	Alto	Pode acontecer algumas vezes
4	Muito Alto	Praticamente certo que irá acontecer, e vai repetir-se

1.Níveis de avaliação - Impacto (Processo de desenvolvimento)

Nivel	Impacto	Descrição de impacto
1	Baixo	Um posto de trabalho afetado / Uma cliente afetado
2	Médio	Mais que um posto de trabalho afetado / Mais que cliente afetado
3	Alto	Afetou o ambiente de desenvolvimento, mas pode ser reposto / Afetou um cliente mas a informação pode ser reposta
4	Muito Alto	Comprometeu todo o processo de desenvolvimento / Afetou todos os clientes

1.Níveis de avaliação - Impacto (Conformidade contratual)

Nivel	Impacto	Descrição de impacto
1	Baixo	Falha pontual que pode comprometer o serviço
2	Médio	Falha repetida no cumprimento do serviço, sem penalização
3	Alto	Falha repetida no cumprimento do serviço, com penalização
4	Muito Alto	Falhas graves no cumprimento do serviço, com penalização e/ou que comprometam o contrato

1.Níveis de avaliação (impacto)

Impacto / Probabilidad	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

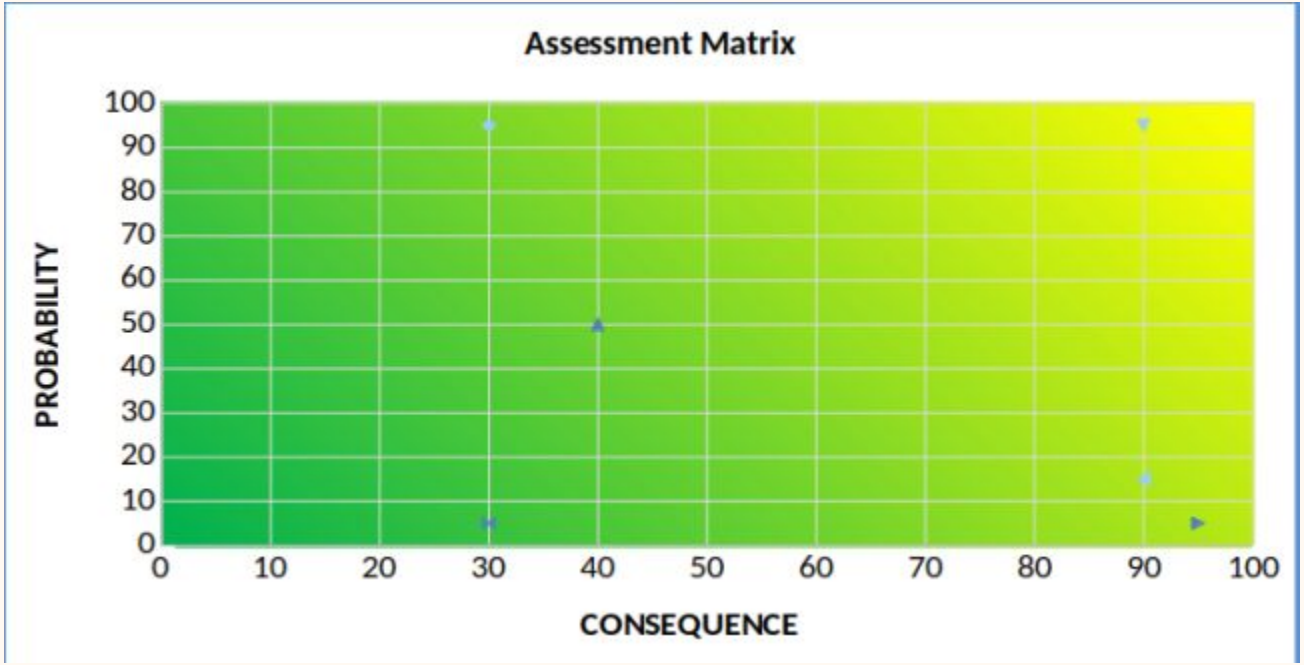
2.Níveis de avaliação (Probabilidade)

Nivel	Probabilidade	Descrição de impacto
1	<10%	Muito improvável
2	10%-35%	Improvável
3	36%-50%	Possível
4	51%-60%	Provável
5	61%-90%	Muito provável
6	>90%	Ocorre sempre

2.Níveis de avaliação (impacto)

Nivel	Impacto	Descrição de impacto
1	<10%	Insignificante, facilmente controlado durante o decorrer normal das operações, sem custos adicionais
2	10%-25%	Menor, algumas interrupções em operações normais, com custo mínimo
3	26%-50%	Moderado, requer uma alocação de tempo/recursos imediatos com custos moderados
4	51%-75%	Alto, operações são interrompidas muito significativamente e podem começar a falhar
5	> 76%	Crítico, preocupações significativas em conseguir manter operações normais

2.Níveis de avaliação (impacto)



Thanks!

Alguma questão?