PÓS-FRAAP

Segurança e Gestão de Riscos

Universidade de aveiro

Autores:
Guilherme Amaral Ribeiro Pereira: 93134
Diogo Miguel Rocha Amaral: 93228
José Luís Costa: 92996

Índice

Sumário executivo

Lista de participantes do processo

A realização deste processo envolveu elementos da equipa consultora, Guilherme Pereira (Facilitador), José Costa (Escrivão) e Diogo Amaral (Facilitador), assim como membros diretamente envolvidos no sistema de recrutamento que foi analisado, entre eles Daniel Guerreiro (Responsável), Catarina santos (Utilizador do sistema), Fernando Costa (Utilizador de pesquisa), Jorge Santos Silva (Utilizador de pesquisa), João Rodrigues (Tecnico), Luís Amorim (Professor da unidade curricular).

Resumo do âmbito e princípios estabelecidos

1. Resumo de como decorreu o processo

De modo geral o processo realizou-se conforme esperado, sendo que com este foi possível identificar ameaças e controlos a aplicar para as que apresentam maior risco para a organização. Este processo iniciou-se com uma breve reunião inicial (Pre-FRAAP) com o responsável Daniel. Posteriormente foi realizada uma reunião mais extensa que reuniu vários participantes ligados ao projeto. Nesta reunião foi possível identificar um número considerável de ameaças (30), controlos e riscos, contudo foi necessário realizar uma reunião adicional. Consideramos que o processo decorreu de forma positiva.

2. Onde e quando decorreu

Pre-FRAAP: 11 de junho de 2022 pelas 11:00 horas da manhã via zoom
FRAAP: 15 de junho de 2002 entre as 14:00 e 18:00 horas da tarde
25 de junho de 2022 às 10:30 horas da manhã

3. Identificar constrangimento e factos assumidos

O âmbito foi a realização de uma análise e avaliação de risco seguindo o processo FRAAP (processo facilitado de análise e avaliação de risco) ao sistema de recrutamento da empresa iCreate com o intuito de conseguir identificar ameaças e potenciais controlos a ser aplicadas aquelas que apresentam um maior risco à organização através desse sistema. Alguns dos funcionários não estiveram disponibilidade de estar presente durante toda a reunião

Resumo da metodologia

Pre-FRAAP: Reunião de 1 a 1,5 horas com o responsável de negócio. Vão definir as bases de trabalho para as fases seguintes
FRAAP: Dura aproximadamente 4 horas e deve incluir uma equipa mais abrangente que inclua os responsáveis de negócio e da infra-estrutura. Identificar ameaças, vulnerabilidades, impactos e controlos.
Post-FRAAP: Normalmente de 1 a 2 semanas. Análise dos resultados e produção do relatório final.

Resumo das principais conclusões da avaliação

Da aplicação da metodologia FRAAP foi possível identificar 30 ameaças. Sendo que uma delas apresenta um risco elevado, com valor 12, e por isso deve ser tratada:

- Utilização de dados previamente inseridos na plataforma que posteriormente os clientes não queriam que fossem divulgados.

Esta ameaça pode pôr em causa o cumprimento da legislação em vigor (RGPD). Para mais informações, como controlos a aplicar verificar a secção 2 da avaliação de riscos
Foram também identificadas 6 ameaças cujo risco é médio e pode ser tratado. Sendo que mais informação sobre estas e como as mitigar encontram-se na secção 2:

- Possibilidade de um candidato enviar emails com conteúdo malicioso
- Técnicas de social engineering sobre programadores/colaboradores (com objetivo de manipular os dados)
- Perda de serviços de suporte (se os terceiros/subcontratante ficar indisponíveis)
- Falha de acesso à ferramenta devido a falha energéticas no escritório
- Falhas no sistema, não detectadas precocemente por falta de monitorização ativa
- Exposição a ataques e exploração de vulnerabilidades conhecidas, por falta de atualização

Referenciação à restante documentação

Durante o processo todo foram elaboradas algumas apresentações e relatórios:
Apresentação do Pre-FRAAP (“Apresentacao_Pre-FRAAP.pdf”), Relatório do Pre-FRAAP (“Relatorio_Pre-FRAAP.pdf”), Apresentação do FRAAP (“Apresentacao_FRAAP.pdf”) e
Excel "Análise e tratamento de riscos - iCreate - Avaliação de Risco.pdf”)

Conclusões

1. Visão sobre o processo todo

Este trabalho teve como objetivo fazer uma análise e avaliação de risco a um sistema de recrutamento. Do processo resultou, numa primeira fase, um relatório que contém informações necessárias para a reunião FRAAP poder ser realizada.
Posteriormente da reunião FRAAP resultou um ficheiro que contém uma tabela de todas as ameaças, os controlos existentes, o risco calculado, novos controlos identificados e o risco residual.

2. Controlos a considerar e um plano de ação / priorização

Estas são as medidas de tratamento ou mitigação dos riscos mais elevados:
Plano de ação/priorização: 1) Processo automático de atualização de dados; **2)** Criação de uma cláusula de confidencialidade e a sensibilização de empregados; **3)** Verificação periódica com o fornecedor para a devida atualização dos sistemas; **4)** Instalação de um IDS e criação de uma blacklist de endereços e-mails; **5)** Sistema que agregue logs dos serviços e envio automático de avisos **6)** Trabalho remoto e introduzir UPS; **7)** Replicação do serviço noutro contratante. Mais informação na secção de planeamento/priorização.

Metodologia

1. Explicação da metodologia

O FRAAP é uma metodologia que tem como objetivo efetuar de forma mais rápida e eficaz uma análise de risco sobre sistemas ou processos. Esta metodologia está dividida em 3 partes:

Pre-FRAAP: breve reunião inicial que serve de preparação para a reunião FRAAP. Envolve o Gestor de Negócios/processos e o Gestor de Projeto assim como a equipa de consultores. Esta reunião demora cerca de 1 a 1,5h e após esta reunião os resultados esperados são os seguintes:

- Pré-Triagem
- Definição do âmbito
- Diagrama do sistema
- Estabelecimento da equipa
- Requisitos para a sessão FRAAP
- Acordar definições
- Mini-Brainstorming

FRAAP: Principal reunião que dura cerca de 4 horas e que envolve todos os elementos da equipa identificados anteriormente. Após esta reunião os resultados esperados são os seguintes:

- Identificar ameaças
- Identificar controlos existentes
- Calcular riscos
- Identificar novos controlos
- Caracterização de riscos residuais

Post-FRAAP: Realização de um relatório com todas as informações resumidas e compactadas, deve conter um sumário executivo, resumo da reunião da equipa, identificação e priorização de novos controlos para mitigar os riscos identificados, e análise de como decorreu o processo.

2. Como correu o processo

Nesta seção encontra-se uma descrição de como correu o processo nas suas fases, como decorreram as reuniões, o que era esperado, os objetivos alcançados e eventualmente mencionar o trabalho adicional que foi realizado pelos consultores. Este processo contou com a participação dos membros representados na tabela abaixo (Tabela 1), tabela essa que contém para cada participante o nome, contacto e papel que teve no processo.

Nome	Contacto	Função
Guilherme Pereira	guilherme.pereira@ua.pt	Facilitador
Diogo Amaral	diogomra7@ua.pt	Facilitador
José Costa	joselcosta@ua.pt	Escrivão
Daniel Guerreiro	daniel.f.guerreiro@inoweiser.com	Responsável de área de recrutamento e seleção
Catarina Santos	catarina.s.santos@iwoseier.com	Utilizadora do sistema (insere dados)
Fernando Costa	fernando.costa@iw.com	Utilizador de pesquisa
Jorge Santos Silva	jorge.silva@inowiser.com	Utilizador de pesquisa
João Rodrigues	joao.p.rodrigues@icreateconsulting.com	Técnico
Luís Amorim	luisamorim@ua.pt	Professor da unidade curricular e membro da empresa

Tabela 1: Lista de participantes

1. Pre-FRAAP

Conforme mencionado na subseção anterior, o primeiro passo nesta metodologia é a realização de uma reunião inicial.
Com o intuito de conseguir alcançar todos os objetivos da reunião foi preparado uma breve apresentação da metodologia FRAAP assim como propostas para definições de termos e métodos de cálculo de risco.
Foi então elaborada via zoom no dia **11 de junho de 2022 pelas 11:00 horas da manhã** a primeira reunião (pre-FRAAP), onde estiveram presentes todos os elementos da equipa de consultores, assim como o responsável Daniel Guerreiro.
Com o decorrer dessa reunião fomos capazes de atingir a maioria dos objetivos pretendidos, com a exceção da obtenção do diagrama do sistema. Sendo que não foi possível obter o diagrama do sistema, foi acordado no fim da reunião que este seria posteriormente disponibilizado.
Após a reunião ter sido efetuada, foi elaborado um relatório contendo informação acerca de todos os objetivos que foram/tinham de ser alcançados (Relatorio_Pre-FRAAP.pdf). O relatório e os slides desenvolvidos para suporte à reunião foram disponibilizados através de um email ao professor da cadeira assim como ao responsável Daniel Guerreiro.

2. FRAAP

Conforme acordado na reunião pré-fraap foi então realizada no dia **15 de junho de 2002 entre as 14:00 e 18:00 horas da tarde** a reunião fraap via ferramenta zoom. Esta reunião teve participação dos elementos contidos na Tabela 1 deste relatório, com exceção do técnico João Rodrigues.
Com o intuito de conseguir dar suporte à reunião foram elaborados slides de suporte para serem usados durante a reunião.
A reunião começou por uma breve introdução da reunião e da equipa por parte do responsável Daniel Guerreiro, seguida de uma apresentação da agenda e breve introdução da metodologia à equipa por parte dos facilitadores. Não foi possível apresentar o diagrama na reunião devido a falta deste.
Após se terem apresentado as definições previamente acordadas no pré-fraap foram novamente revistos os objetivos. Os facilitadores procederam então à recolha de informação relativa a todos os participantes da reunião assim como a fazer uma revisão de acordos que são necessários para que esta corresse de forma esperada.
Numa segunda parte da reunião foram identificadas por parte dos participantes e com algumas sugestões dos facilitadores ameaças ao sistema de recrutamento SIR. Sendo que a identificação começou pelo atributo da confidencialidade seguindo-se o da integridade e por fim o da disponibilidade.
Com isto foi possível identificar um total de 30 ameaças ao sistema.
Já no final desse processo compreensivelmente alguns participantes tiveram a necessidade de se ausentar por motivos profissionais.
Subsequentemente foram identificados os controlos já existentes para mitigar as ameaças identificadas e foi calculado o risco associado às ameaças com esses controlos. Não foi possível identificar o risco e os controlos para todas as ameaças, pois seria necessário o conhecimento técnico.
Por último foram identificados alguns controlos a implementar aos maiores riscos calculados, sendo que por falta de tempo e de pessoal técnico na reunião não foi possível calcular o risco residual.
De modo a completar os objetivos necessários para a reunião, foi necessário acordar uma reunião extra com o técnico João Rodrigues.
No fim desta reunião foram enviados ao professor da cadeira e ao responsável Daniel o documento excel (“Análise e tratamento de riscos - iCreate - Avaliação de Risco.pdf”) com todas as ameaças identificadas, controlos e riscos assim como os slides de suporte à reunião.

3. FRAAP reunião adicional com o técnico

Foi então realizada uma pequena reunião adicional no dia **25 de junho de 2022 às 10:30 horas da manhã** uma reunião adicional com o professor da cadeira e o técnico João Rodrigues. Esta reunião teve como objetivo responder algumas questões que ficaram em aberto na reunião realizada no dia 15.
Com esta reunião ficou apenas a faltar o cálculo do risco residual e a identificação de novos controlos para as ameaças que tinham ficado em aberto.

4. Post-FRAAP

Em relação à última fase da metodologia foi desenvolvido este relatório com o intuito de apresentar todos os resultados obtidos, assim como identificar o planeamento e priorização dos controlos a implementar.

Avaliação de riscos

Foram denotadas 30 ameaças identificadas com a ajuda dos participantes, mas apenas 7 delas devem ser mitigadas, o que indica que a empresa já apresenta algum nível de segurança.
Nesta secção vamos abordar numa primeira fase essas 7 ameaças cujo risco é médio/ elevado, identificando o valor desse risco e os controlos existentes.
Posteriormente, na segunda parte, encontram-se novos controlos a aplicar para mitigar o risco.
Referir que a lista de todas as 30 ameaças identificadas, incluindo aquelas que apresentam um nível de risco aceitável, encontra-se disponível no excel em anexo (Análise e tratamento de riscos - iCreate - Avaliação de Risco.pdf).

NOTA: Nas tabelas seguintes o ID corresponde ao ID atribuído no ficheiro de excel que resultou da reunião FRAAP.

1. Ameaças

O cálculo do risco seguirá a fórmula (Risco X Probabilidade), o que vai de acordo com a seguinte tabela.
Para elaborar a avaliação foi tido em conta a matriz de cálculo de risco previamente acordada com a empresa na reunião Pre-FRAAP, assim como o uso das tabelas que atribuem um nível ao impacto e a probabilidade.

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

1.1 Confidencialidade

De seguida encontram-se todas as ameaças identificadas que põem em causa o atributo de confidencialidade.

ID	Ameaças	Controlos já implementados	Risco
3	Possibilidade de um candidato enviar emails com conteúdo malicioso	Existe anti-spam e antivírus para filtragem de emails no servidor de correio; Antivirus defender instalado em todas as máquinas	6
4	Utilização de dados inseridos que mais tarde os candidatos não pretendem que sejam divulgados.	-	12

Tabela 2: Ameaças de confidencialidade

Como podemos ver aqui se encontra a ameaça que apresenta maior risco para a organização (ameaça com ID 4), visto que ela pode levar a um incumprimento do regulamento geral de proteção de dados. Um dos direitos desse regulamento, que pode estar em causa, é o direito ao esquecimento (Artigo 17º Direito ao apagamento dos dados <direito a ser esquecido>).

1.2 Integridade

De seguida encontram-se todas as ameaças identificadas que põem em causa a integridade dos dados e do sistema.

ID	Ameaças	Controlos já implementados	Risco
14	Técnicas de social engineering sobre programadores/colaboradores (com objetivo de manipular os dados dados)	-	8

Tabela 3: Ameaças de integridade

1.3 Disponibilidade

De seguida encontram-se todas as ameaças identificadas que põem em causa o atributo da disponibilidade.

ID	Ameaças	Controlos já implementados	Risco
25	Perda de serviços de suporte (se os terceiros/subcontratante ficar indisponíveis)	-	8
28	Falha de acesso à ferramenta devido a falha energéticas no escritório	-	6
30	Falhas no sistema, não detectadas precocemente por falta de monitorização ativa	Monitorização diária de ocupação do disco	6

Tabela 4: Ameaças de disponibilidade

1.4 Ameaças que afetam mais que um atributo

Por último encontram-se as ameaças encontradas que põem em causa mais que um atributo de segurança.

ID	Ameaças	Tipo	Controlos já implementados	Risco
18	Exposição a ataques e exploração de vulnerabilidades conhecidas, por falta de atualização	CIA	Contratualizado com fornecedor	8

Tabela 5: Ameaças de vários atributos

2. Controlos a implementar

Nesta seção encontram-se os controlos a implementar que foram identificados para as ameaças que apresentam um risco elevado ou um risco que pode ser mitigado (médio).
Esta informação pode também ser encontrada no excel com a informação obtida na reunião FRAAP.

ID	Ameaça	Controlos a implementar	Novo nível de risco
3	Possibilidade de um candidato enviar emails com conteúdo malicioso	Instalação de um IDS (intrusion detection system); Criação de uma blacklist para endereços email que já tenham enviado conteúdo malicioso anteriormente	3
4	Utilização de dados inseridos que mais tarde os candidatos não pretendem que sejam divulgados	Automatização de atualização de dados através de um requerimento; Garantir o consentimento formal do candidato	4
14	Técnicas de social engineering sobre programadores/colaboradores (com objetivo de manipular os dados dados)	Cláusula de confidencialidade; Sensibilização dos empregados	3
18	Exposição a ataques e exploração de vulnerabilidades conhecidas, por falta de atualização	Verificação periódica com o fornecedor para garantir a atualização periódica dos sistemas	3
25	Perda de serviços de suporte (se os terceiros/subcontratante ficar indisponíveis)	Compra e implementação de serviços em servidores redundantes noutro subcontratante, por exemplo (Amazon Web Services AWS)	2
28	Falha de acesso à ferramenta devido a falha energéticas no escritório	Trabalho Remoto e UPS	2
30	Falhas no sistema, não detectadas precocemente por falta de monitorização ativa	Implementar um sistema que agregue logs dos vários serviços; Envio automático de avisos quando os recursos atingirem um certo threshold.	2

Tabela 6: Controlos a implementar

Planeamento/priorização

Com o intuito de mitigar o risco que as ameaças apresentam à organização foi necessário identificar controlos, contudo isto não é suficiente. Após terem sido identificados é necessário traçar uma ordem pela qual estes controlos devem ser implementados, não só pelo risco que as ameaças apresentam mas também pelo tempo, potencial custo financeiro, eficiência/benefício que estas apresentam. Para os controlos identificados colocámos uma referência para o capítulo genérico do controlo segundo a norma ISO 27001, no entanto é preciso ter em conta que só é referenciado o capítulo visto que a norma é paga e não é possível verificar o conteúdo.
De seguida encontram-se os controlos que devem ser implementados por ordem. Começando pela ameaça que apresenta maior risco, pois esta leva a um incumprimento da lei, seguindo-se a sensibilização e a cláusula de confidencialidade pela facilidade/benefício que esta apresenta. As restantes estão ordenadas pelo esforço de implementação e custo monetário inerentes.

1. Ordem

1.1 Primeira implementação

ID da ameaça: **4**

Ameaça: Utilização de dados inseridos que mais tarde os candidatos não pretendem que sejam divulgados.

Controlo: Deve ser automatizado o processo de atualização de dados através de um requerimento e garantir o consentimento formal do candidato, de forma a que os dados do cliente inseridos na plataforma não possam ser posteriormente divulgados.

ISO: ISO 27001 Annex A.18 – Compliance + alinhamento com RGPD: (Artigo 17º Direito ao apagamento dos dados <direito a ser esquecido>).

1.2 Segunda implementação

ID da ameaça: **14**

Ameaça: Técnicas de social engineering sobre programadores/colaboradores (com objetivo de manipular os dados dados).

Controlo: Para diminuir o risco da utilização de técnicas de social engineering sobre programadores/colaboradores, é necessário a criação de uma cláusula de confidencialidade e a sensibilização de empregados.

ISO: ISO 27001 A.7.2 Information Security Awareness

1.3 Terceira implementação

ID da ameaça: **18**

Ameaça: Exposição a ataques e exploração de vulnerabilidades conhecidas, por falta de atualização.

Controlo: Para diminuir o risco dos sistemas não se encontram devidamente atualizados, deve ser efetuada uma verificação periódica com o fornecedor para a devida atualização.

ISO: ISO 27001 A.12.6.1 Gestão de vulnerabilidades técnicas.

1.4 Quarta implementação

ID da ameaça: **3**

Ameaça: Possibilidade de um candidato enviar emails com conteúdo malicioso.

Controlo: Deve ser instalado um IDS (intrusion detection system) e uma blacklist para endereços de email que já tenham enviado conteúdo malicioso anteriormente, de forma a prevenir que o candidato envie emails com conteúdo malicioso.

ISO: ISO 27001 A.12.2.1 Controlos contra código malicioso.

1.5 Quinta implementação

ID da ameaça: **30**

Ameaça: Falhas no sistema, não detectadas precocemente por falta de monitorização ativa.

Controlo: Para diminuir o risco de existirem falhas em serviços devido a falta de monitorização dos servidores, deve ser implementado um sistema que agregue logs dos vários serviços e envie automaticamente avisos de quando os recursos atingirem um certo threshold.

ISO: ISO 27001 A.12.1.3 Gestão da capacidade, A.12.4.1 Registos de eventos

1.6 Sexta implementação

ID da ameaça: **28**

Ameaça: Falha de acesso à ferramenta devido a falha energética no escritório.

Controlo: Para diminuir o risco de existir falhas de acesso à ferramenta devido a falha energética no escritório, pode ser implementado trabalho remoto através da

disponibilização da plataforma de forma segura (remotamente). Além disso, podem ser introduzidas UPS para mitigar durante algum tempo a falha energética.

ISO: ISO 27002 A.11.2.2 Serviços básicos de suporte.

1.7 Sétima Implementação

ID da ameaça: **25**

Ameaça: Perda de serviços de suporte (se os terceiros/subcontratantes ficarem indisponíveis).

Controlo: Para diminuir os risco da perda de serviços de suporte por terceiros ficarem indisponíveis, deve ser replicado o serviço noutro subcontratante, criando assim redundância do serviço. (Amazon Web Services por exemplo)

ISO: ISO 27001, Annex A.17.2 redundancy, A.17.1 Aspectos da segurança da informação na gestão da continuidade do negócio

2. Riscos residuais

O risco residual encontra-se na tabela 6 da secção dos controlos a implementar e no excel em anexo.
Referir que a probabilidade e impacto usado no cálculo deste novo risco pode ser encontrado também nesse excel disponibilizado Análise e tratamento de riscos - iCreate - Avaliação de Risco.pdf").

Conclusões

Desde já agradecemos a contribuição e disponibilidade do professor, da empresa ICreate e de todos os colaboradores durante todo o processo da metodologia FRAAP.
Utilizando os diferentes passos desta metodologia foi possível elaborar uma análise de risco no qual foram identificadas várias ameaças, calculados riscos, e encontrados controlos para os que permitam mitigar os maiores riscos para a organização.
Foram identificados 30 ameaças, para as quais 7, devido ao seu risco inerente, necessitam de identificação de controlos adicionais. Conforme mencionado no relatório existe uma ameaça que apresenta um risco elevado à empresa pois pode pôr em causa o comprimento de legislação em vigor pelo que é fortemente recomendado que a mesma seja mitigada através da implementação dos controlos identificados.
Dito isto, de modo geral pensamos ter atingido os objetivos propostos para esta análise, sendo que, se estes controlos forem implementados será incrementada a segurança da organização.