Universidade de aveiro

Pré-FRAAP

Mestrado em Cibersegurança
Segurança e Gestão de Riscos

Autores:

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

2021/2022

Índice

Objetivo

A análise e avaliação de risco é um processo fundamental nos dias que decorrem no contexto empresarial. Não só devido ao facto de os sistemas serem cada vez mais extensos e complexos, mas por outro lado também pelo facto de haver um aumento de potenciais ameaças contra as infraestruturas.

Tendo em consideração o mencionado anteriormente foi-nos proposta 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.

À luz dessa metodologia o objetivo deste relatório é apresentar a informação que foi obtida na primeira fase do método, designada Pré-FRAAP, que envolveu o responsável pelo projeto, Daniel Guerreiro assim como a equipa de consultores.

Referências

ISO/IEC 27001:2013 - Especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da organização.

ISO/IEC 27002:2013 - Fornece diretrizes para padrões organizacionais de segurança da informação e práticas de gestão de segurança da informação, incluindo a seleção, implementação e gestão de controlos tendo em consideração o(s) ambiente(s) de risco de segurança da informação da organização.

ISO/IEC 27005:2013 - Fornece diretrizes para o gerenciamento de riscos de segurança da informação. Isto apoia os conceitos gerais especificados no ISO/IEC 27001 e é desenhado para auxiliar a implementação satisfatória da segurança de informação com base numa abordagem de gerenciamento de risco.

Regulamento Geral de Proteção de Dados (RGPD) - O Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679 é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu que foi criado em 2018. Regulamenta também a exportação de dados pessoais para fora da União Europeia e o Espaço Econômico Europeu. O RGPD tem como objetivo dar aos cidadãos e residentes formas de controlar os seus dados pessoais e unificar o quadro regulamentar europeu.

National Institute of Standards and Technology (NIST) - É uma agência governamental não regulatória da administração de tecnologia dos Estados Unidos. Tem como missão promover a inovação e a competitividade industrial dos Estados Unidos com a definição de bons padrões e correta utilização de tecnologias.

Âmbito

O âmbito deste projeto é uma análise e avaliação de risco utilizando a metodologia FRAAP ao SIR (sistema interno de recrutamentos) da empresa iCreate.

Diagrama do sistema

Em relação ao diagrama do sistema, ficou acordado na reunião que o mesmo seria posteriormente disponibilizado. Desse modo, o mesmo não consta neste relatório.

Equipa a incluir no processo

No que toca à equipa a incluir no processo, não foi possível detalhar todos os colaboradores e utilizadores a incluir, sendo que a indicação dos mesmo será posteriormente fornecida.

Os elementos que até ao momento deste relatório foram confirmados encontram-se na seguinte tabela

Nome	Função	Contacto email
Guilherme Pereira	Facilitador	guilherme.pereira@ua.pt
Diogo Amaral	Facilitador	diogomra7@ua.pt
José Costa	Escriba	joselcosta@ua.pt
Daniel Guerreiro	Responsável pelo projeto	daniel.f.guerreiro@inoweiser.com

Tabela1: Nome e contactos dos participantes

Requisitos reunião FRAAP

A realização da reunião FRAAP ficou marcada para às 14:00 **horas** do dia **15 de junho de 2022** e terá uma duração de cerca de **4 horas**, prevendo -se assim que acabe às **18:00 horas.**

A reunião será realizada através da ferramenta zoom, sendo que o link da reunião irá ser disponibilizado posteriormente.

Definições

1.Termos técnicos

Nome	Descrição
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.

Tabela 2: Termos técnicos

2. Avaliação de riscos

2.1 Probabilidade

Nível	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

Tabela 3: Probabilidade

2.2 Impacto (Processo de recrutamento)

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

Tabela 4: Processo de desenvolvimento

2.3 Impacto (Conformidade contratual)

Nível	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

Tabela 5: Termos conformidade contratual

2.4 Cálculo do risco

O cálculo do risco seguirá a fórmula (Risco X Probabilidade), o que vai de acordo com a seguinte tabela.

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

Tabela 6: Cálculo de risco

Mini-Brainstorming

O mini-brainstorming foi realizado com o objetivo de identificar algumas ameaças que posteriormente vão ser utilizadas como exemplos na introdução para facilitar a reunião FRAAP.

No mini-brainstorming realizado as ameaças identificadas foram as seguintes:

Confidencialidade:

- No caso de um indivíduo não autorizado adquirir credenciais de acesso na plataforma SIR é possível aceder a todos os dados da mesma.
- Os dados fornecidos pelo cliente podem potencialmente ser usados para questões de marketing.

Integridade:

- Os dados dos candidatos podem não se encontrar devidamente atualizados na base de dados.

Confidencialidade, Integridade e Disponibilidade:

- Emails com conteúdos maliciosos podem ser enviados por qualquer pessoa para o email das candidaturas.