FERRAMENTA EXCEL CRAM

Um guia passo a passo

A Matriz de Auditoria em Cibersegurança (CRAM) é uma ferramenta analítica para apoiar as empresas de fabrico a identificar, analisar, priorizar riscos e estabelecer medidas de proteção eficazes.

Este guia resumido tem como objetivo ajudar na aplicação da ferramenta Excel CRAM. Por favor, leia o Manual da CRAM antes!

A CRAM inclui:

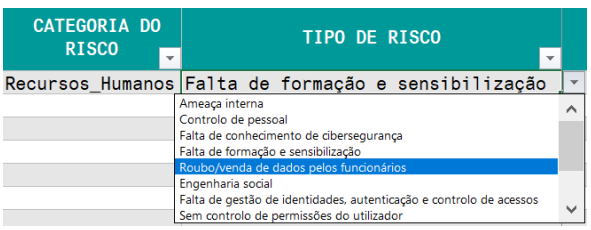
- **número do risco** definido previamente, apenas para ajudar na identificação do risco.

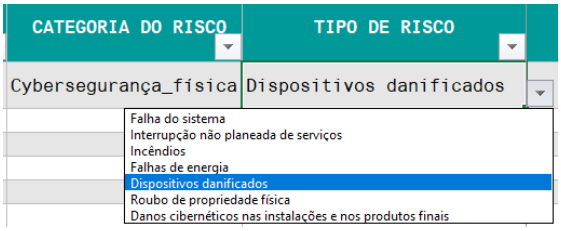
- **categoria do risco**

Selecione na ferramenta a categoria de risco, a descrição das categorias é apresentada no Manual da CRAM.

- **tipo de risco**

De acordo com a categoria selecionada, a ferramenta CRAM irá sugerir-lhe o respetivo tipo de risco.

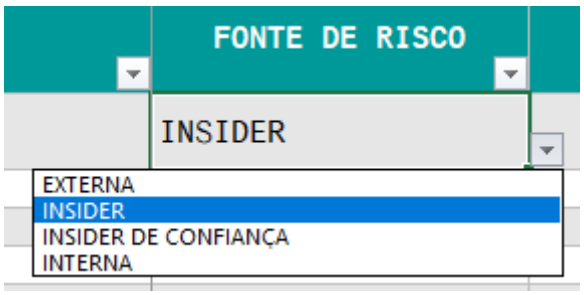




Em alguns tipos de risco, há uma lista suspensa onde pode encontrar mais riscos para além dos que estão visíveis, como no primeiro exemplo apresentado.

- **Fonte do risco**

Selecione a fonte do risco: Externa, Insider, Insider de Confiança, Interna.



Fonte de risco	Descrição
EXTERNA	Ataques de forças externas originados no ambiente digital.
INSIDER	Uma ameaça causada por um funcionário que usa o acesso autorizado, intencionalmente ou não, para prejudicar a segurança da empresa.
INSIDER DE CONFIANÇA	É alguém que tenha tido acesso aos sistemas e instalações físicas de uma empresa. Isto inclui antigos empregados, fornecedores, clientes, parceiros de negócios, visitantes ou outros terceiros.
INTERNA	Fonte interna (hardware, network, software, organizacional).

- **descrição do risco**

Campo aberto para a descrição do risco. Isto ajudará a definir melhor o risco e os próximos passos do processo.

* Se o Tipo de Risco for "Problemas de Integridade de Dados", por favor inclua o seguinte tipo de dados na "Descrição do Risco"

PROBLEMAS DE INTEGRIDADE DOS DADOS
dados digitais de alto nível
dados digitais de baixo nível
dados financeiros
dados físicos
dados do utilizador

- **custos potenciais associados às consequências do risco**

Campo aberto para identificar todos os custos potenciais associados às consequências de o risco acontecer. Ex: valor monetário relacionado com roubo de informação de propriedade ou fraude financeira; custos relacionados com perda severa de uso ou produtividade incluem vírus e malware, Ataques de rejeição de serviço do servidor web, abuso de privilégios de acesso, e vandalismo de equipamentos ou roubo…

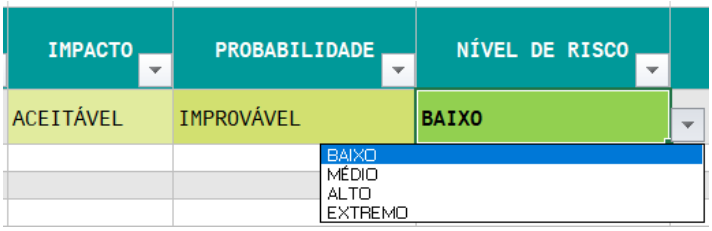
- **departamentos da organização que podem ser afetados**

Campo aberto para identificar o(s) departamento(s) da organização que podem ser afetados.

- **medidas preventivas/ações previamente implementadas**

Campo aberto para identificar e descrever as medidas preventivas/ações previamente implementadas (se aplicável).

- **Avaliação e cálculo de elementos de risco** (impacto do risco, probabilidade do risco, nível global do risco)



Entradas relativas à probabilidade (isto é, a probabilidade de ocorrer um risco) e o impacto (isto é, a gravidade do risco em caso de ocorrência) dos riscos identificados. É classificada a probabilidade e o impacto com uma escala de Baixo (0), Médio (1), Alto (2) e Extremo (3).

NÍVEL DO RISCO	BAIXO 0 - Aceitável OK PARA CONTINUAR	MÉDIO 1 - Moderado FAZER ESFORÇOS DE MITIGAÇÃO	ALTO 2 - Geralmente Inaceitável PROCURAR APOIO - implementar ações em 6 meses	EXTREMO 3 - Intolerável COLOCAR PROCEDIMENTO EM ESPERA

	IMPACTO			
	ACEITÁVEL Pouco a nenhum efeito	TOLERÁVEL Os efeitos são sentidos, mas sem resultado crítico	INDESEJÁVEL Impacto sério no decurso da ação e no resultado	INTOLERÁVEL Pode resultar em desastre
PROBABILIDADE				
IMPROVÁVEL Pouco provável que o risco ocorra	BAIXO 1	MÉDIO 4	MÉDIO 6	ALTO 10
POSSÍVEL O risco provavelmente ocorrerá	BAIXO 2	MÉDIO 5	ALTO 8	EXTREMO 11
PROVÁVEL O risco vai ocorrer	MÉDIO 3	ALTO 7	ALTO 9	EXTREMO 12

- **trigger (elemento impulsionador)**

Campo aberto para descrever os impulsos ou ações que fazem com que o sistema inicie uma resposta. O trigger deve ser um alerta para quando ocorre um incidente ou comportamento anómalo.

- **mitigação/ações a implementar**

Campo aberto para a identificação de ações de mitigação para os riscos qualificados de Médio a Alto. Isto significa tentar eliminar ou reduzir a frequência, magnitude ou gravidade da exposição aos riscos, ou minimizar o potencial impacto de uma ameaça.

No Manual CRAM estão identificados dois tipos de controlos de ação – preventivas e corretivas em cada uma das nove categorias de risco.

- **potenciais custos da mitigação**

Campo aberto para a identificação dos potenciais custos da mitigação.

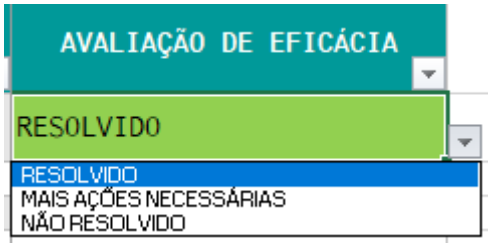
- **prazo**

Prazo para as ações a implementar.

- **responsabilidade**

Campo aberto para a identificação do responsável pela gestão de risco e do supervisor responsável pela monitorização.

- **avaliação de eficácia**



A CRAM Encrypt 4.0 é composta por um processo sistemático e contínuo. É um processo cíclico que uma vez identificado, analisado, avaliado, tratado e aceite o risco, deve realizar-se um processo de monitorização e revisão de riscos. Caso o problema persista, terá de aplicar mais ações complementares para resolver o problema, e para isso, terá de voltar ao passo anterior ao tratamento de risco. E se o problema não for resolvido, terá de reavaliar o risco.

- **relatório**

Depois de preencher todos os campos necessários, tem o seu relatório de risco concluído.

O Projeto ENCRYPT4.0 (2020-1-RO01-KA202-079983) foi financiado com o apoio da Comissão Europeia. Esta publicação reflete apenas os pontos de vista do autor e a Comissão não pode ser responsabilizada por qualquer utilização que possa ser feita das informações contidas.