

Registro de Riscos

Ambiente operacional:

O banco está localizado em uma área costeira com baixos índices de criminalidade. Muitas pessoas e sistemas lidam com os dados do banco — 100 funcionários presenciais e 20 funcionários remotos. A base de clientes do banco inclui 2.000 contas individuais e 200 contas comerciais. Os serviços do banco são divulgados por um time profissional de esportes e dez empresas locais da comunidade. Existem regulamentações financeiras rigorosas que exigem que o banco proteja seus dados e fundos, como manter dinheiro suficiente disponível diariamente para atender aos requisitos do Federal Reserve.

Ativos	Risco(s)	Descrição	Probabilidade	Severidade	Prioridade
Fundos	Comprometimento de e-mail comercial	<i>Um funcionário é enganado a compartilhar informações confidenciais.</i>	2	3	6
	Banco de dados de usuários comprometido	<i>Os dados dos clientes estão mal criptografados</i>	3	3	9
	Vazamento de registros financeiros	<i>Um servidor de banco de dados com dados de backup está publicamente acessível.</i>	3	3	9
	Roubo	<i>O cofre do banco é deixado destrancado.</i>	1	3	5
	Interrupção da cadeia de suprimentos	<i>Atrasos na entrega devido a desastres naturais.</i>	1	2	3
Notas	Os possíveis eventos de segurança podem ocorrer porque muitos funcionários e sistemas manipulam dados sensíveis, o que aumenta consideravelmente a chance de erros humanos ou ataques direcionados. Além disso, a presença de operações remotas e servidores acessíveis amplia a superfície de ataque para criminosos. Fatores ambientais, como desastres naturais, também podem interromper a cadeia de suprimentos e afetar a segurança financeira.				

Ativo: O ativo em risco de ser prejudicado, danificado ou roubado.

Risco(s): Um risco potencial aos sistemas de informação e dados da organização.

Descrição: Uma vulnerabilidade que pode levar a um incidente de segurança.

Probabilidade: Pontuação de 1 a 3 sobre as chances de uma vulnerabilidade ser explorada.

1 = baixa probabilidade, 2 = probabilidade moderada, 3 = alta probabilidade.

Severidade: Pontuação de 1 a 3 do potencial dano que a ameaça causaria ao negócio.

1 = baixo impacto, 2 = impacto moderado, 3 = alto impacto.

Prioridade: Com que rapidez o risco deve ser tratado para evitar o incidente potencial.

Fórmula: **Probabilidade × Severidade = Risco**

Exemplo de matriz de risco

		Severidade		
Probabilidade		Baixa (1)	Moderada (2)	Catastrófica (3)
	Certa (3)	3	6	9
	Provável (2)	2	4	6
	Rara (1)	1	2	3