SECRETARIA DE ESTADO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GERÊNCIA DE APOIO ADMINISTRATIVO E LOGÍSTICO

MATRIZ DE RISCOS

Introdução

A análise de riscos é o processo de compreender a natura e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento do risco da aquisição da ***Renovação do Suporte e garantia Firewall Fortinet****. O risco é uma função tanto da probabilidade como da medida das consequências. Desse modo, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos. O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco.* **Referencial básico de Gestão de Riscos, Tribunal de Contas da União (TCU) , 2018**

Risco é o efeito da **incerteza sobre objetivos estabelecidos**. É a possibilidade de ocorrência de eventos que **afetem a realização ou alcance dos objetivos**, combinada com o impacto dessa ocorrência **sobre os resultados pretendidos**.

Gestão de riscos consiste em um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. É o processo que visa **conferir razoável segurança quanto ao alcance dos objetivo**s.

Para a análise de risco será utilizado o método qualitativo, que define o **impacto versus probabilidade** e, também o nível da escala de risco por qualificadores numéricos que determinarão o **método qualitativo como:** BAIXO, MÉDIO, ALTO, EXTREMO, facilitando com base na percepção das pessoas para análise. A relação entre os riscos e os seus componentes pode ser ilustrada por meio de uma matriz que se correlaciona com as variantes impacto e probabilidade; segue-se a imagem abaixo:

Figura 01 - Matriz de riscos simples

Utilizando-se da matriz de **PROBABILIDADE x IMPACTO**, imagem abaixo, conforme orientação do comitê de compliance desta Secretaria, temos a seguinte Matriz de Probabilidade x Impacto:

Matriz de Probabilidade x Impacto							
Impacto	16	Catastrófico	16	32	48	64	80
	8	Maior	8	16	24	32	40
	4	Moderado	4	8	12	16	20
	2	Menor	2	4	6	8	10
	1	Desprezível	1	2	3	4	5
			Raro	Improvável	Possível	Provável	Quase Certo
			1	2	3	4	5
			Probabilidade				

Escala de Níveis de Risco (Nível de Risco = Peso Prob. x Peso Impacto)		
Escala	**De**	**Até**
Baixo	1	4
Médio	5	9
Alto	10	30
Extremo	31	80

Figura 02 - Matriz de riscos - Probabilidade x Impacto

A avaliação dos riscos deve seguir os seguintes passos:

- Identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a aquisição como um todo;
- Identificar os riscos que estão abaixo do limite de exposição;
- Identificar, na matriz probabilidade x impacto, os riscos cujos níveis estão acima do limite de exposição ao risco (faixa vermelha da matriz)
- Para os riscos cujos níveis se encontram na faixa amarela deverá ser avaliada a necessidade de monitoramento;
- Os riscos cujos níveis se encontram na faixa verde poderão ser aceitos.

Com base na análise de riscos e na sua classificação, os riscos identificados estão alinhados com o plano de gestão da matriz riscos da Secretaria e são assim classificados: **PROBABILIDADE BAIXA** e **IMPACTO MÉDIO**. Como forma de mitigar o impacto dos riscos supramencionados seria de extrema relevância a aquisição.

Objeto

A contratação contempla a subscrição de garantia e suporte técnico especializado para firewall e soluções de gerenciamento, assegurando, a proposta inclui serviços de atualizações, suporte técnico integral e manutenção, por um período de 36(trinta e seis)meses.

Lote	Item	Quantidade	Serviço
01	01	06	Renovação de garantia e suporte FortiCare Premium com subscrição FortiGuard UTP Protection (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Anti-spam), por 36(trinta e seis) meses para equipamentos FortiGate 1101E.
	02	01	Renovação de garantia e suporte FortiCare Premium com subscrição para até 30 VDOMs, por 36(trinta e seis) meses para FortiManager VM.

Mapa de Riscos

Subscrição de garantia e suporte técnico especializado para firewall e soluções de gerenciamento									
Seq.	**Nome do Risco**	**Descrição do Risco**	**Impacto**	**Consequências**	**Probabilidade**	**Classificação do Risco**	**Responsáveis**	**Descrição da Resposta**	**Data para Ação**
1	Atraso na Licitação	Atraso no início do processo de licitação do serviço.	Alto	Prejuízo na continuidade da proteção de rede e aumento da vulnerabilidade.	Média	Alto	Equipe de Compras	Planejamento antecipado e cronograma definido com prazos.	Imediata
2	Demora na Assinatura do Contrato	Tempo excessivo para assinatura do contrato após o processo licitatório.	Médio	Atraso na implementação do serviço, prejudicando a proteção da rede.	Alta	Médio	Jurídico/Compras	Acompanhamento constante e mitigação de entraves burocráticos.	Imediata
3	Licitação Deserta	Ausência de interessados no processo de licitação.	Alto	Necessidade de reinício do processo licitatório, causando atrasos significativos.	Média	Alto	Equipe de Compras	Ampliar a divulgação e revisar requisitos do edital.	Curto Prazo
4	Falha no Firewall	Interrupção total da segurança da rede por falha no firewall instalado.	Alto	Acesso não autorizado, roubo de dados, paralisação dos serviços de rede.	Média	Alto	Equipe de TI	Implementar suporte imediato e atualização proativa para correção de falhas.	Imediata
5	Atraso na Resolução de Incidentes	Tempo excessivo para solucionar problemas devido à falta de suporte especializado.	Médio	Tempo ocioso, prejuízo operacional e insatisfação de usuários.	Alta	Médio	Fornecedor/TI	Garantir SLA com suporte técnico de nível 24x7 e especializado.	Imediata
6	Falta de Atualizações de Segurança	A ausência de patches e atualizações compromete a segurança do firewall.	Alto	Vulnerabilidades exploradas, invasão de sistemas e roubo de dados sensíveis.	Média	Alto	Equipe de TI	Contratar subscrição de suporte técnico com atualizações frequentes.	Contínua
7	Ameaças de Cyberataques	Aumento de ameaças virtuais sem suporte eficaz para prevenção.	Alto	Perda de dados, paralisação de sistemas e danos à reputação da organização.	Alta	Alto	Fornecedor/TI	Utilização de soluções de gerenciamento robustas e suporte 24x7.	Imediata
8	Falha de Integração com Sistemas	Problemas de compatibilidade do firewall com outras soluções de rede.	Médio	Redução do desempenho da rede e interrupção de sistemas integrados.	Baixa	Médio	Equipe de TI	Realizar testes prévios de compatibilidade e integração.	Contínua
9	Ausência de Monitoramento Contínuo	Falta de visibilidade constante das atividades e possíveis ameaças no sistema.	Alto	Detecção tardia de ameaças, comprometendo a segurança dos sistemas.	Média	Alto	Fornecedor/TI	Implementar solução de monitoramento contínuo com suporte especializado.	Imediata

Conclusão da Análise de Riscos

A análise dos riscos demonstrou que os **impactos associados à falta de suporte técnico especializado** para firewall e soluções de gerenciamento são significativos, com **classificações predominantes entre Médio e Alto risco**. Destacam-se riscos de falhas operacionais, ameaças de ciberataques e a perda de segurança de dados críticos.

Portanto, a **contratação deste serviço é essencial** para garantir a **continuidade operacional**, a **proteção contra ameaças externas** e a **eficiência na gestão da segurança da rede**. Além disso, contribui para a **redução de incidentes críticos**, garantindo maior estabilidade e produtividade à organização.