GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

1 OBJETIVO

Estabelecer o processo de gestão de riscos de segurança da informação (PGRSI).

2 APLICAÇÃO

O escopo de aplicação do PGRSI é definido pelos demais processos que dele fazem uso. Por exemplo, o PGRSI pode ser demandado para:

a) **estabelecer ou revisar o Sistema de Gestão de Segurança da Informação**;

b) **integrar o processo de gestão de riscos corporativos**, quando detectada a necessidade de investigar riscos em ativos de informação que fazem parte do escopo de determinado processo de trabalho;

c) **gerenciar riscos em ativos envolvidos em processo de mudança significativa**: mudança contextual ou aquisição, desenvolvimento, modificação e desativação de um ou mais ativos de informação;

3 REFERÊNCIA NORMATIVA

3.1 PO01 – Política de Segurança da Informação e Comunicação do TRT18.

3.2 RA 78/2019 – Política de Gestão de Riscos.

3.3 PLGR – Plano de Gestão de Riscos, conforme Portaria TRT18 GP/SGGOVE nº 2618/2019.

3.4 Norma ABNT NBR ISO/IEC 27005:2018 (Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação).

4 DEFINIÇÕES

Para efeito desta norma, são adotadas as definições descritas nesta seção e nos documentos PO01 e PLGR.

4.1 **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em um dano para um sistema ou organização.

4.2 **Ativo de Informação**: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

4.3 **Controle**: forma de gerenciar o risco, incluindo diretrizes, políticas, normas, procedimentos, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

4.4 **Vulnerabilidade**: fragilidade de um ativo de informação (do ponto de vista da segurança), ou de um controle, que pode ser explorada por uma ameaça.

5 METODOLOGIA

5.1 O PGRSI está alinhado ao documento RA 78/2019, adotando entretanto, em função de suas especificidades, a metodologia de gestão de riscos presente na ferramenta Módulo Risk Manager, compatível com a versão 9.8.

5.2 Os critérios de risco utilizados neste processo estão descritos no anexo III – Estabelecimento do Contexto Geral do documento PLGR.

5.3 Na metodologia incorporada na ferramenta Módulo Risk Manager, cada ativo de informação, ou simplesmente “ativo”, é avaliado quanto à sua **relevância** para a organização (**R**, numa escala de 1 a 5).

5.4 Um ativo está associado a um ou mais componentes de ativo. Por exemplo, o ativo “Banco de Dados” pode integrar os componentes de ativo “máquina virtual VMware”, “sistema operacional RedHat” e “sistema de banco de dados Oracle”.

5.5 Cada componente de ativo está associado a uma lista de riscos denominada *Knowledge Base (KB)*, que se assemelha a uma lista de verificação de controles aplicáveis à mitigação desses riscos.

5.6 A ferramenta disponibiliza um conjunto de *Knowledge Bases* para

componentes de ativos dos tipos tecnologia, processos, pessoas e ambientes, e permite também que sejam adicionadas *KBs* personalizadas.

5.7 A relação "causa-evento-consequência" de cada controle (risco identificado) na *Knowledge Base* é descrita em termos de "Justificativa" do controle e mensurada em termos de **probabilidade** de ocorrência (**P**, numa escala de 1 a 5) e **severidade** das consequências sobre o ativo (**S**, numa escala de 1 a 5).

5.8 Numa relação previamente identificada entre ativos e componentes de ativos, o nível de risco para cada controle não aplicado é calculado pela fórmula "RISCO = PxSxR", sendo "P" a dimensão probabilidade e "SxR" a dimensão impacto.

5.9 A conversão dos níveis de riscos sobre ativos (PSR) para o critério "Matriz de Classificação de Riscos" do TRT18 (constante no PLGR e definida pela relação Impacto x Probabilidade), ocorre fazendo-se a seguinte verificação sequencial: BAIXO para PSR < 15; MÉDIO para PSR < 40; ALTO para PSR < 75; EXTREMO para PSR > ou = 75.

5.10 As opções selecionadas para tratamento dos riscos são previamente descritas em termos de "Recomendação" para a implementação de cada controle listado nas *Knowledge Bases*.

5.11 Uma vez aplicado um controle, não há apuração do respectivo risco residual.

5.12 O risco residual considerado para cada ativo refere-se aos controles a ele associados e que não foram aplicados, uma vez que seus riscos puderam ser aceitos em conformidade com o critério "Apetite a Riscos" indicado no documento PLGR, ou seja, risco classificado como ACEITÁVEL ou OPORTUNIDADE (PSR < 40, ou ainda, riscos MÉDIOS ou BAIXOS).

6 PROCESSO

O PGRSI compreende a execução das seguintes atividades principais: Estabelecer escopo, contexto e critérios, Identificar riscos, Analisar riscos, Avaliar riscos, Tratar riscos, Monitorar e analisar criticamente, Comunicar e consultar e Registrar e relatar.

6.1 Estabelecer escopo, contexto e critérios

6.1.1 Finalidade: obter do PLGR e do processo demandante o conjunto de informações necessárias para identificar e inventariar os ativos de informação

(escopo), compreender o ambiente interno e externo de ameaças a esses ativos (contexto) e observar os critérios de risco que deverão ser utilizados ao longo do processo (critérios).

6.1.2 Responsável: Gestor de Riscos.

6.2 Identificar riscos

6.2.1 Finalidade: identificar (ou atualizar) nas bases de conhecimentos de riscos do TRT18 as boas práticas de segurança da informação ou de gestão de riscos que são recomendadas para aplicação em cada componente de ativo presente no escopo.

6.2.2 Responsável: Responsável pelo Ativo, pessoa designada pelo Gestor de Riscos.

6.3 Analisar riscos

6.3.1 Finalidade: estimar a probabilidade e a severidade de cada risco identificado, assim como o respectivo nível (PSR).

6.3.2 Responsável: Responsável pelo Ativo.

6.4 Avaliar riscos

6.4.1 Finalidade: obter uma lista de riscos priorizadas para tratamento, a partir da comparação dos níveis de riscos estimados com os critérios para aceitação de riscos (apetite a riscos).

6.4.2 Responsável: Gestor de Riscos.

6.5 Tratar riscos

6.5.1 Elaborar Plano de Tratamento de Riscos:

a) Finalidade: elaborar um plano de tratamento de riscos, a partir de uma análise de custo/benefício sobre lista de riscos priorizados, e submetê-lo à implementação;

b) Responsável: Gestor de Riscos.

6.5.2 Implementar o Plano de Tratamento de Riscos:

a) Finalidade: implementar os controles estabelecidos no Plano de Tratamento de Riscos;

b) Responsável: Responsável pelo Ativo.

6.6 Monitorar e analisar criticamente

6.6.1 Finalidade: aprimorar o processo e seus resultados a partir do monitoramento

e da análise crítica de todas as suas atividades.

6.6.2 Responsável: Comissão de Segurança da Informação, com suporte da unidade de apoio à governança de Tecnologia da Informação e Comunicação.

6.7 Comunicar e consultar

6.7.1 Finalidade: manter fluxo regular e constante de informações com as partes interessadas, durante todas as atividades do processo.

6.7.2 Responsável: Gestor de Riscos.

6.8 Registrar e relatar

6.8.1 Finalidade: documentar o processo e seus resultados; relatar tais resultados às partes interessadas; apoiar as atividades das instâncias internas de governança.

6.8.2 Responsável: Gestor de Riscos.

7 INDICADORES

7.1 Risk Index: percentual de projetos de riscos que atingiram a meta de Risk Index no período de apuração. Risk Index refere-se aos riscos não controlados (“aceitos” + “em tratamento”) / risco a controlar (total dos riscos identificados)

7.2 Controles Implementados: percentual de controles implementados dentro do prazo estabelecido para conclusão do projeto de riscos.

8 DISPOSIÇÕES GERAIS

8.1 O Anexo I apresenta o fluxo do PGRSI, onde as atividades “Comunicar e Consultar” e “Registrar e Relatar” estão ausentes para fins de simplificação do diagrama.

8.2 Esta norma entrará em vigor a partir de sua publicação e deverá ser revisada anualmente.

Anexo I

Fluxo do Processo de Gestão de Riscos de Segurança da Informação