Análise de Riscos

Versão 1.0
Abril de 2024

CONTROLE DE VERSÃO

Versão	Data	Nome	Ação
1.0	16/04/2024	LUÍS CARLOS SNOLDO VIANA	Elaboração

Sumário

INTRODUÇÃO

Esta **Análise de Riscos** é composta por cinco partes: **Recurso protegido, Vulnerabilidade, Ameaças, Avaliação do risco e Tratamento**.

São fases do gerenciamento de riscos:

a) identificação dos recursos a serem protegidos – hardware, rede, software, dados, informações pessoais, documentação e suprimentos;

b) identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);

c) análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

d) avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;

e) tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

f) monitoração da eficácia dos controles adotados para minimizar os riscos identificados;

g) reavaliação periódica dos riscos em intervalos de tempo não superiores a um ano.

Os recursos protegidos são os ativos da AR que deverão ser resguardados de quaisquer riscos. A vulnerabilidade indica as situações em que os recursos protegidos podem ser expostos e suscetíveis a danos. As ameaças expõem os principais riscos aos quais a AR poderá estar exposta e a avaliação do risco apresenta os indicadores de impacto, probabilidade e grau das principais ameaças, sem considerar as ações gerenciais que possam reduzir a probabilidade de sua ocorrência.

As Ameaças estão identificadas pelo código e descrição. O código está relacionado ao risco levantado na descrição.

A Avaliação do risco está classificado por impacto, probabilidade e grau do risco.

O impacto da avaliação do risco é classificado como insignificante, baixo, médio, alto e crítico. Essa escala é assim mensurada, quando há degradação de operações ou atividades de processos:

Grau do Impacto

- **Grau 1 - insignificante:** impacto irrelevante nos objetivos.
- **Grau 2 - baixo:** impacto pequeno.
- **Grau 5 - médio:** impacto significativo, porém recuperável.
- **Grau 8 - alto:** impacto de reversão muito difícil.
- **Grau 10 - crítico:** impacto irreversível e catastrófico.

Probabilidade

A probabilidade também está escalonada em insignificante, baixa, média, alta e crítica:

- **Grau 1 - insignificante:** evento improvável de ocorrer.
- **Grau 2 - baixa:** evento raro de ocorrer. Poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.
- **Grau 5 - média:** evento possível de ocorrer. Há elementos ou informações que indicam moderadamente essa possibilidade.
- **Grau 8 - alta:** evento provável de ocorrer. É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.
- **Grau 10 - crítica:** evento praticamente certo de ocorrer. Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.

Grau do risco

O risco é classificado como baixo, médio, alto e extremo. Essa escala é assim mensurada:

- **Graus de 1 a 9** – risco baixo
- **Graus de 10 a 39** – risco médio
- **Graus de 40 a 79** – risco alto
- **Graus de 80 a 100** – risco extremo.

Estimativa do risco

Calcula-se a avaliação do risco aplicando-se a fórmula:

- **(Avaliação do risco) = (grau do impacto) x (grau da probabilidade)**.

Os controles adotados para minimizar os riscos identificados deverão ser monitorados eficazmente e o tempo para reavaliação periódica dos riscos não poderá ser superior a um ano.

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Recurso protegido

Acesso às instalações da AR

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Permissão de acesso à instalação técnica da AR a pessoas não autorizadas.	346	Vulnerabilidade geral	Alto	Insignificante	8	Baixo	Eliminar

Dados

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Coleta biométrica ilegível	119	Perda de dados e Informações	Baixo	Baixa	4	Baixo	Eliminar
Equipamentos de computação sem a devida proteção contra vírus, trojan, spyware e outras ameaças virtuais.	114	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de armazenamento local dos logs de auditoria por período mínimo de 60 dias.	124	Perda de dados e Informações	Alto	Insignificante	8	Baixo	Eliminar
Falta de definição de perfil de acesso aos equipamentos e recursos da AR com permissões e restrições de acordo com o tipo de usuário.	111	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de identificação e autenticação dos usuários autorizados a acessar equipamentos e recursos da AR.	109	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de logs de auditoria para registro de acessos aos equipamentos.	123	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Falta de proteção contra modificações não autorizadas nos equipamentos e recursos da AR.	112	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de proteção de senhas com grau de segurança compatível com a informação associada.	113	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de revogação das credenciais, identificações e acessos lógicos de AGR desligado ou suspenso.	108	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de sistema de controle de acesso aos equipamentos e recursos da AR ou habilitações desatualizadas.	110	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar

Firewall ativado com permissões de acesso além do necessário para a realização das atividades.	116	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Firewall desativado.	115	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar

Dados e informações pessoais

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Estações de trabalho sem utilização de fonte confiável do tempo (FCT) para data e hora.	122	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Falta de formalização e confirmação de habilitação e desabilitação de AGR no sistema de certificação da AC	328	Responsabilidade Administrativa, Cível e Criminal	Alto	Insignificante	8	Baixo	Eliminar

Documentação

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Falta de comunicação à AC de qualquer alteração nos atos constitutivos, estatuto, contrato social ou administradores da AR.	347	Responsabilidade Administrativa, Cível e Criminal	Baixo	Insignificante	2	Baixo	Eliminar
Arquivamento dos documentos digitalizados que compõem o dossiê do titular do certificado fora do ponto de centralização preestabelecido.	306	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Ausência de assinatura digital padrão ICP-Brasil nos documentos digitalizados que compõem o dossiê do titular do certificado.	102	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Ausência de documentação comprobatória do treinamento dos AGRs	325	Insuficiência de prova	Baixo	Insignificante	2	Baixo	Eliminar
Dificuldade de localizar qualquer dossiê de titular de certificado que se encontra sob a guarda AR	315	Perda de documentos físicos	Baixo	Insignificante	2	Baixo	Eliminar
Falta da guarda da cópia do PCN em local seguro fora da sala da AR	342	Perda de documentos físicos	Alto	Insignificante	8	Baixo	Eliminar
Falta de armazenamento em dossiê dos documentos de AGR em atuação na AR.	329	Insuficiência de prova	Médio	Insignificante	5	Baixo	Eliminar
Falta de armazenamento em dossiê dos documentos de AGR que já aturaram AR e não atuam mais.	330	Insuficiência de prova	Médio	Insignificante	5	Baixo	Eliminar

Falta de atualização mensal do inventário de todos os ativos da AR.	337	Responsabilidade Administrativa, Cível e Criminal	Baixo	Insignificante	2	Baixo	Eliminar
Falta de backup dos documentos digitalizados	105	Perda de dados e Informações	Alto	Insignificante	8	Baixo	Eliminar
Falta de especificação dos procedimentos de cópias e recuperação dos documentos digitalizados em caso de sinistro.	314	Perda de dados e Informações	Alto	Insignificante	8	Baixo	Eliminar
Falta de histórico das alterações do inventário de ativos devidamente assinado pelo responsável pela instalação técnica ou posto provisório da AR.	338	Responsabilidade Administrativa, Cível e Criminal	Baixo	Insignificante	2	Baixo	Eliminar
Falta de implementação do PCN	339	Perda de controle do negócio	Alto	Insignificante	8	Baixo	Eliminar
Falta de organização dos arquivos que compõem o dossiê do titular do certificado de forma a permitir recuperação conjunta para fins de fiscalização e auditoria.	313	Perda de documentos físicos	Baixo	Baixa	4	Baixo	Eliminar
Falta de revisão do processo de gerenciamento de risco a cada 18 meses no máximo.	341	Responsabilidade Administrativa, Cível e Criminal	Alto	Insignificante	8	Baixo	Eliminar
Janelas abertas no momento de vendavais	210	Dispersão	Alto	Insignificante	8	Baixo	Eliminar
Manutenção de documentos que compõem o dossiê dos titulares de certificado em ambiente fora do ponto de centralização preestabelecido.	301	Exposição indevida de dados e informações pessoais	Médio	Insignificante	5	Baixo	Eliminar
Manutenção de documentos que compõem o dossiê dos titulares de certificado em arquivo não chaveado dentro do ponto de centralização preestabelecido.	303	Exposição indevida de dados e informações pessoais	Médio	Insignificante	5	Baixo	Eliminar
Remessa ou transmissão do dossiê do titular de certificado digital em prazo superior a 30 dias corridos	317	Perda de documentos físicos	Baixo	Insignificante	2	Baixo	Eliminar

Documentação e informações pessoais

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Falta de proteção contra leitura e gravação do diretório ou sistema onde são armazenados os documentos digitalizados do dossiê do titular do certificado.	103	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Falta de verificação da solicitação por AGR distinto do que executou a etapa de validação	310	Fraude	Médio	Insignificante	5	Baixo	Eliminar

Falta de verificação da solicitação por AGR distinto do que executou a etapa de validação	310	Fraude	Médio	Insignificante	5	Baixo	Eliminar
Verificação em segundo nível realizada fora das instalações técnicas da AR	311	Responsabilidade Administrativa, Cível e Criminal	Alto	Insignificante	8	Baixo	Eliminar
Verificação em segundo nível realizada fora das instalações técnicas da AR	311	Responsabilidade Administrativa, Cível e Criminal	Alto	Insignificante	8	Baixo	Eliminar

Duplo vínculo de AGR

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
AGR vinculado a mais de uma AR	345	Deparar com vínculo de AGR a outra AR sem conhecimento prévio e concordância	Alto	Insignificante	40	Alto	Eliminar
AGR vinculado a mais de uma AR	346	Permitir o vínculo de AGR já vinculado a outra AR	Baixo	Média	5	Baixo	Mitigar

Hardware e Software

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Ambiente computacional não auditável utilizado para validação do processo de solicitação e revogação de certificados fora da AR	101	Fraude	Médio	Insignificante	5	Baixo	Transferir as perdas
Ambiente computacional não registrado no inventário de hardware e software da AR utilizado para validação do processo de solicitação e revogação de certificados fora da AR	307	Fraude	Médio	Insignificante	5	Baixo	Eliminar
Falta de proteção dos circuitos elétricos de alimentação dos equipamentos de processamento de dados por no-break ou estabilizador de tensão.	204	Curto circuito e destruição e danificação de equipamentos eletrônicos	Médio	Insignificante	5	Baixo	Eliminar
Sistema Operacional desatualizado ou sem aplicação de correções de patches, hotfix, etc, necessários.	118	Ataque cibernético	Alto	Insignificante	8	Baixo	Eliminar
Utilização de software não licenciado.	120	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar

Informações pessoais

Vulnerabilidade	Ameaças		Risco Inerente			Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco	

Falta da apresentação de documentos originais no ato de solicitação e revogação de certificados	304	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Falta de conferência dos dados da solicitação de certificado com os documentos originais apresentados	309	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Falta de confirmação da identidade do cliente no ato de solicitação e revogação de certificados.	305	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Remessa do dossiê do titular de certificado digital para armazenamento definitivo por meio não seguro.	316	Roubo, perda, destruição e danificação de documentos físicos	Alto	Insignificante	8	Baixo	Eliminar
Solicitação de certificados e de revogação não presencial	302	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Termo de titularidade sem assinatura do candidato ou titular PF, ou do representante legal da PJ	308	Fraude	Alto	Insignificante	8	Baixo	Eliminar
Transmissão do dossiê do titular de certificado digital para armazenamento definitivo por meio não seguro.	106	Roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Transporte do dossiê do titular de certificado digital para armazenamento definitivo por meio não seguro.	107	Roubo, perda, destruição e danificação de documentos físicos	Alto	Insignificante	8	Baixo	Eliminar

Instalação técnica

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Abalos sísmicos	201	Desmoronamento	Alto	Insignificante	8	Baixo	Eliminar
Ausência de iluminação de emergência.	207	Vulnerabilidade geral	Médio	Insignificante	5	Baixo	Eliminar
Ausência de proteção dos circuitos elétricos e lógicos por tubulação e/ou canaletas adequadas.	205	Incêndio e curtocircuito	Médio	Insignificante	5	Baixo	Eliminar
Falta de atendimento de requisitos de segurança da instalação técnica nos pontos de centralização dos dossiês de titulares de certificados	202	Agressão Física, Roubo, perda, destruição e danificação de documentos físicos, móveis e equipamentos, Exposição indevida de dados e informações pessoais	Alto	Insignificante	8	Baixo	Eliminar
Falta de equipamento de prevenção de incêndio.	203	Incêndio	Alto	Insignificante	8	Baixo	Eliminar
Falta de fechadura com mecanismo de segurança mais sofisticado que modelos simples na porta de acesso à AR.	206	Roubo, destruição e danificação de toda espécie de bens físicos	Alto	Insignificante	8	Baixo	Eliminar
Janelas abertas no momento de temporais	209	Inundação	Alto	Baixa	16	Médio	Eliminar
Porta de acesso à instalação técnica destrancada	211	Vulnerabilidade geral	Alto	Insignificante	8	Baixo	Eliminar

Torneiras abertas nas dependências da instalação técnica no momento de falta d'água.	208	Inundação	Baixo	Baixa	4	Baixo	Eliminar

Rede

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Permissão de login remoto, exceto para atividades de suporte remoto regularmente permitidas.	121	Fraude, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar

Rede, dados e informações pessoais

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Ataques de hakers, invasões e outros ataques típicos de engenharia social	125	Ataque cibernético, roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar

Segurança da informação

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Acesso de pessoas não permitidas aos dossiês dos titulares de certificados e dos AGRs.	343	Exposição indevida de dados e informações pessoais	Alto	Insignificante	8	Baixo	Eliminar
Ausência de treinamento de novos AGRs em princípios e mecanismos da segurança da informação.	320	AGR desatualizado profissionalmente	Alto	Insignificante	8	Baixo	Eliminar
Documentos mantidos na AR e armazenados em armários ou gabinetes sem chave ou de uso não exclusivo da AR.	345	Exposição indevida de dados e informações pessoais	Alto	Insignificante	8	Baixo	Eliminar
Falta de atualização dos AGRs sobre eventuais mudanças tecnológicas nos sistemas da AC	322	AGR desatualizado profissionalmente	Baixo	Baixa	4	Baixo	Eliminar
Falta de atualização dos AGRs sobre eventuais mudanças tecnológicas nos sistemas da AR	321	AGR desatualizado profissionalmente	Médio	Insignificante	5	Baixo	Eliminar
Falta de revogação das credenciais, identificações e acessos físicos de AGR desligado ou suspenso.	336	Vulnerabilidade geral	Alto	Insignificante	8	Baixo	Eliminar
Falta de teste anual do PCN	340	Perda de controle do negócio	Médio	Insignificante	5	Baixo	Eliminar
Falta de treinamento dos novos AGRs em reconhecimento de assinaturas e validade de documentos	323	AGR desatualizado profissionalmente	Alto	Insignificante	8	Baixo	Eliminar

Falta de treinamento dos novos AGRs no sistema de certificação em uso na AC	324	AGR desatualizado profissionalmente	Alto	Insignificante	8	Baixo	Eliminar
Sistema de eliminação de mídias desnecessárias não seguro e fora dos procedimentos de eliminação.	344	Roubo, destruição e corrupção de documentos eletrônicos, informações e dados	Alto	Insignificante	8	Baixo	Eliminar
Estação de trabalho sem proteção de tela, proteção não ativada, ou ativada em desconformidade com as recomendações e exigências.	117	Exposição indevida de dados e informações pessoais	Alto	Insignificante	8	Baixo	Eliminar

Segurança jurídica

Vulnerabilidade	Ameaças		Risco Inerente				Tratamento do Risco
	Cód.	Descrição	Impacto	Probabilidade	Grau do Risco		
Ausência de acompanhamento de desempenho dos AGRs	318	Responsabilidade Administrativa, Cível e Criminal	Alto	Insignificante	8	Baixo	Eliminar
Ausência de avaliação anual dos AGRs	319	AGR desatualizado profissionalmente	Médio	Insignificante	5	Baixo	Eliminar
Falta de comprovante de residência do AGR	335	Insuficiência de prova	Alto	Insignificante	8	Baixo	Eliminar
Falta de documentação da entrevista de admissão de AGR.	332	Insuficiência de prova	Médio	Insignificante	5	Baixo	Eliminar
Falta de histórico de empregos anteriores do candidato a AGR.	333	Insuficiência de prova	Médio	Insignificante	5	Baixo	Eliminar
Falta de registro em contrato ou termo de responsabilidade do perfil da função que o AGR desempenhará.	334	Insuficiência de prova	Médio	Insignificante	5	Baixo	Eliminar
Falta de renovação anual ou bienal dos antecedentes criminais e da situação de crédito dos AGRs, conforme definido nas normas da ICP-Brasil.	327	AGR inadequado por insuficiência de requisitos	Alto	Insignificante	8	Baixo	Eliminar
Falta de suspensão de AGR que praticar ação não autorizada e de instauração de processo administrativo para apurar sua responsabilidade.	331	Vulnerabilidade geral	Alto	Insignificante	8	Baixo	Eliminar
Falta de verificação de antecedentes criminais e situação de crédito dos novos AGRs em processo de admissão.	326	AGR inadequado por insuficiência de requisitos	Alto	Insignificante	8	Baixo	Eliminar
Não revogação automática de certificado emitido com início de validade futura sem que a verificação ocorra antes do início da validade.	312	Fraude	Alto	Baixa	16	Médio	Eliminar

MAGNITUDE DE IMPACTOS E PROBABILIDADES

Magnitude de impactos

Escala de Impactos		
Magnitude	**Descrição**	**Impacto**
Muito baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causando **impactos mínimos nos objetivos** de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos pequenos nos objetivos**.	2
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando **impactos significativos nos objetivos, porém recuperáveis.**	5
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando **impactos de reversão muito difícil nos objetivos.**	8
Muito alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos irreversíveis/catastróficos nos objetivos.**	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (Adaptada)

Magnitude de probabilidades

Escala de Probabilidades		
Magnitude	**Descrição**	**Impacto**
Muito baixa	**Evento improvável de ocorrer.** Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade.	1
Baixa	**Evento raro de ocorrer.** O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	2
Média	**Evento possível de ocorrer.** Há elementos e/ou informações que indicam moderadamente essa possibilidade.	5
Alta	**Evento provável de ocorrer.** É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	8
Muito alta	**Evento praticamente certo de ocorrer.** Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (adaptada)

ESCALA DE IMPACTOS, PROBABILIDADES E RISCO

Escala de Impactos	
Impacto	**Grau**
Insignificante	1
Baixo	2
Médio	5
Alto	8
Crítico	10

Escala de Probabilidades	
Probabilidade	**Grau**
Insignificante	1
Baixa	2
Média	5
Alta	8
Crítica	10

Escala do Risco	
Grau	**Nível**
1	Baixo
2	Baixo
3	Baixo
4	Baixo
5	Baixo
6	Baixo
7	Baixo
8	Baixo
9	Baixo
10	Médio
11	Médio
12	Médio
13	Médio
14	Médio
15	Médio
16	Médio
17	Médio
18	Médio
19	Médio
20	Médio
21	Médio
22	Médio
23	Médio
24	Médio
25	Médio
26	Médio
27	Médio
28	Médio
29	Médio
30	Médio
31	Médio
32	Médio
33	Médio
34	Médio
35	Médio
36	Médio
37	Médio
38	Médio
39	Médio
40	Alto

41	Alto
42	Alto
43	Alto
44	Alto
45	Alto
46	Alto
47	Alto
48	Alto
49	Alto
50	Alto
51	Alto
52	Alto
53	Alto
54	Alto
55	Alto
56	Alto
57	Alto
58	Alto
59	Alto
60	Alto
61	Alto
62	Alto
63	Alto
64	Alto
65	Alto
66	Alto
67	Alto
68	Alto
69	Alto
70	Alto
71	Alto
72	Alto
73	Alto
74	Alto
75	Alto
76	Alto
77	Alto
78	Alto
79	Alto
80	Extremo
81	Extremo
82	Extremo
83	Extremo
84	Extremo
85	Extremo

86	Extremo
87	Extremo
88	Extremo
89	Extremo
90	Extremo
91	Extremo
92	Extremo
93	Extremo
94	Extremo
95	Extremo
96	Extremo
97	Extremo
98	Extremo
99	Extremo
100	Extremo