MANUAL DO PROCESSO GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Gerência de Outsourcing TI |GOI

São Paulo – 2022

Versão 1.0

Portfólio

Operação de Outsourcing - Secretaria Estadual da Saúde

Assessoria

Berli Garcia Filho

Superintendente

Jorge Antônio Weschenfelder

Gerência

Jobson Nunes

Coordenação

David Ramos

Liderança

Julia Souza Pimenta

SUMARIO

1. OBJETIVO

Definir o Processo de Gestão de Riscos de Segurança da Informação, da Operação de Outsourcing - Secretaria de Estado da Saúde (SES S. Paulo).

2. ESCOPO

Este processo tem como propósito definir a gestão de riscos de Segurança da Informação da Operação de Outsourcing - Secretaria de Estado da Saúde (SES S. Paulo), garantindo que os riscos sejam conhecidos, monitorados e tratados, promovendo a manutenção de um nível de risco aceitável.

3. DEFINIÇÕES

Para efeitos deste manual, aplicam-se as definições da Política de Segurança da Informação e Comunicações, além das seguintes:

- **Risco:** fator ou evento incerto que pode causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos; ou positivos, com potencial de agregar valores;
- **Risco de Segurança da Informação:** probabilidade de impacto negativo nos objetivos da organização caso as suas informações não estejam protegidas adequadamente;
- **Gestão de riscos:** conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos;
- **Gestão de riscos de Segurança da Informação:** gestão de riscos aplicada ao escopo da Segurança da Informação;

Tolerância ao risco ou apetite de risco: é a quantidade de risco que a instituição está propensa a aceitar para alcançar seus objetivos, podendo definir ainda níveis de desvio aceitáveis no desempenho de suas atividades;

- **Controle:** qualquer medida que visa minimizar um risco ou grupo de riscos;
- **Nível ou índice de risco**: magnitude de um risco ou combinação de riscos;
- **Identificação de riscos:** etapa da gestão de riscos que visa localizar, listar e caracterizar os riscos;
- **Análise de riscos:** etapa da gestão de riscos que visa compreender a natureza dos riscos e determinar o nível de risco. A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos. A análise de riscos inclui a estimativa de riscos;
- **Avaliação de riscos:** etapa da gestão de riscos onde são definidos quais os riscos identificados na análise serão aceitos ou tratados, bem como priorizar o tratamento dos mesmos;
- **Tratamento de riscos:** etapa da gestão de riscos onde são implementadas ações e controles visando reduzir o nível de risco para um patamar aceitável;
- **Relatório de Análise de Riscos (RAR):** apresenta, de forma consolidada, o resultado da análise de riscos;
- **Relatório Operacional de Riscos (ROR):** apresenta o detalhamento das ações e controles que devem ser implementados para eliminar ou mitigar os riscos;
- **Plano de Tratamento de Riscos (PTR):** descreve as ações de tratamento de riscos, identificando os responsáveis, com o objetivo de reduzir os riscos a níveis aceitáveis.

4. POLÍTICAS E DIRETRIZES

Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas, sejam elas da Secretaria de Estado da Saúde (SES S. Paulo), ou por ela custodiadas, visando a garantia de sua Disponibilidade, Integridade, Confidencialidade e Autenticidade.

Prover uma orientação e apoio da direção para a Segurança da Informação de acordo com os requisitos do negócio, com as leis e regulamentações vigentes e aplicáveis, e com as melhores práticas e frameworks de mercado, como por exemplo, a ABNT NBR ISO/IEC 27001:2013.

As orientações aqui apresentadas são os princípios fundamentais e representam como a Secretaria de Estado da Saúde (SES S. Paulo), exige que a informação seja utilizada e protegida em toda a sua cadeia de valor, estabelecendo assim princípios e valores estratégicos a serem adotados pela função informática, e atendendo as atividades fim, em aderência com a missão da Secretaria de Estado da Saúde (SES S. Paulo).

Nossa Norma de Política de Segurança da Informação está disponível na rede, no caminho mencionado abaixo:

\\nas\NAS\CPS\GIS\CIC\PRODESP-Outsourcing\PROCESSOS SES\GERENCIAMENTO\6Gerenciamento Segurança da Informação\Normas

5. FLUXO DO PROCESSO

Fluxo do processo de gestão de riscos da segurança da informação, disponível no caminho na rede descrito abaixo:

\\nas\nas\CPS\GIS\CIC\PRODESP-Outsourcing\PROCESSOS SES\GERENCIAMENTO\6Gerenciamento Segurança da Informação\Gerenciamento de riscos

6. ENTRADAS E SAÍDAS

As principais entradas e saídas do Processo de Gestão de Riscos de Segurança da Informação são:

6.1.Entradas

Escopo do SGSI (Sistema de Gestão de Segurança da Informação) definido pelo CGSI (Comitê Gestor da Segurança da Informação);

Inventário de Ativos.

6.2.Saídas

Relatório de Análise de Riscos – RAR;

Relatório Operacional de Riscos – ROR;

Plano de Tratamento de Riscos;

Relatório de Execução do Plano de Tratamento de Riscos – RE.

7. DESCRIÇÃO DAS PRINCIPAIS ATIVIDADES DO PROCESSO

Apresentar a situação atual da infraestrutura do Data Center Secretaria de Estado da Saúde (SES S. Paulo), bem como seus potenciais de riscos e recomendações relacionadas aos ambientes de:

- Rede e Segurança;
- Banco de dados;
- Sistemas operacionais;

- Infraestrutura;

7.1.Garantias

Para os ativos que possuem informações sobre a data de término da garantia, estas devem ser obtidas nos sites dos fabricantes através do número serial presente fisicamente nos equipamentos. Para os ativos que não possuem informação sobre a data de término da garantia, estas deverão ser obtidas através das empresas contratadas para suporte adicional ou através dos fabricantes mediante a apresentação de nota fiscal ou ordem de compra.

7.2.Redes

7.2.1.Solução Switches

Os ativos relacionados neste item são responsáveis pela efetiva interoperabilidade entre a rede de campus e de data center. Também são responsáveis pela conectividade de entrada e saída com links de dados e acesso externo aos serviços fornecidos pela secretaria.

7.2.2.Núcleo

Os switches de núcleo estão empilhados e são gerenciados através de um IP único formando uma solução redundante de núcleo de rede. São responsáveis pela centralização de todo o tráfego de rede de Campus e Data Center. Os servidores estão conectados a switches de topo de rack (TOR), que por sua vez estão conectados ao core redundante.

7.2.3.Top of Rack (TOR)

Os switches Top of Rack (TOR) são responsáveis pela interconexão entre todos os ativos existentes num determinado rack e o switch núcleo ou distribuição em uma rede. Os switches DELL estão configurados em pilhas de 2 e 4 switches atendendo ao Data Center de forma redundante

7.2.4.Acesso

Os switches de acesso são utilizados para conexão de todos os equipamentos e dispositivos de rede utilizados pelos usuários, tais como, desktops, notebooks, telefones, impressoras, entre outros.

7.2.5.Endereçamento de Rede

Os endereços IP normalmente são expressos em formato decimal com pontos, com quatro números separados por pontos, como 192.168.123.132. Para entender como as máscaras de sub-rede são usadas para distinguir entre hosts, redes e sub-redes, examine um endereço IP em notação binária.

7.2.6.Solução Wireless

A solução Wireless disponível na secretaria é composta por uma controladora virtualizada no ambiente de cluster do VMWare e 52 (cinquenta e dois) Access Points distribuídos pelo ambiente, permitindo o gerenciamento centralizado de suas funcionalidades.

]

7.2.7.Solução Firewall

A Solução de Firewall é responsável pela proteção, controle e confidencialidade de todo o tráfego das aplicações e serviços mantidos pelo data center ou acessados pelos usuários que estão em um ambiente externo.

7.2.8.Solução Software (Gerenciamento e Monitoramento)

A Secretaria de Estado da Saúde (SES S. Paulo), dispões de soluções para o monitoramento SNMP e armazenamento dos LOGs dos dispositivos de redes, wireless e de segurança. Além disso conta com solução específica (Zabbix) para monitoramento de ativos de rede, servidores, e serviços hospedados no Data Center.

7.2.9.Links de Comunicação

Os links de comunicação existentes em produção são todos contratados pela secretaria através do projeto Intragov e ao longo dos anos foram realizados upgrades de capacidade à medida que as demandas do data center aumentavam.

7.3.Banco de Dados

Apresentar a situação atual da infraestrutura de bancos de dados relacionada à SESSP, bem como seus potenciais riscos e recomendações relacionadas ao ambiente, serão citados os serviços de SQL SERVER, MySQL, POSTGRESQL e ORACLE.

7.3.1.Solução SQL Server

A Secretaria de Estado da Saúde (SES S. Paulo) dispõe de um cenário que contempla 3 servidores no DC interno, sendo eles 2 de produção e 1 destinado à homologação e 1 servidor de produção alocado no DC Prodesp no modelo PaaS.

7.3.2.Solução MYSQL

A Secretaria de Estado da Saúde (SES S. Paulo) dispõe de um cenário que contempla 13 (treze) servidores MySQL, alocados tanto no DC SES ou DC Prodesp. Esses servidores atendem aos ambientes de produção, homologação e desenvolvimento.

7.3.3.Solução Postgres

Secretaria de Estado da Saúde (SES S. Paulo), dispõe de um cenário que contempla 8 (oito) servidores PostgreSQL que estão distribuídos entre o DC SES e o DC Prodesp, sendo 5 (cinco) de produção e 3 (três) destinados à homologação e desenvolvimento.

7.3.4.Solução Oracle

A Secretaria de Estado da Saúde (SES S. Paulo), dispõe de um cenário que contempla 12 (doze) servidores ORACLE entre o DC SES e o DC Prodesp, sendo 07 (sete) de produção e 04 (quatro) destinados à homologação e 01 (um) de desenvolvimento.

7.4. Storage

Atualmente, estas soluções são responsáveis pelas principais áreas de armazenamento de informações existentes na Secretaria de Estado da Saúde (SES S. Paulo):

Primeira: para a solução de virtualização e serviços instalados diretamente em servidores físicos;
Segunda: para o armazenamento de backup em disco de todo o Datacenter e a terceira solução para atender a solução de virtualização.

7.5.Backup

Atualmente, esta solução é responsável pelo backup e restore das informações existentes na Secretaria de Estado da Saúde (SES S. Paulo) relacionados às rotinas e serviços mantidos no Datacenter, tais como, arquivos de usuários, máquinas virtuais e banco de dados.

7.6.Infraestrutura Rack

Apresentar os principais equipamentos que compõem um rack tais como:

- Bandejas: Sendo os principais acessórios para racks de servidor. ...
- Separadores, organizadores e guias de cabo.
- Dissipadores de ar e sistema de ventilação. ...
- Calha de tomadas. ...
- Outros acessórios

7.7.Plataforma de Virtualização

A plataforma de virtualização para servidor existente no Datacenter Secretaria de Estado da Saúde (SES S. Paulo) é composta por solução específica de gerenciamento centralizado, responsável pelo fornecimento de segurança, performance e escalabilidade;

7.7.1.Servidores de Rack e Cluster VMWARE

Estes ativos são responsáveis pela hospedagem da solução de virtualização VMware ESXi estruturado em Cluster a fim de manter a funcionalidade de alta disponibilidade dos serviços na Secretaria de Estado da Saúde (SES S. Paulo).

7.7.2.Servidores de rack do Cluster de File Server

Estes ativos são responsáveis pela solução de File Server estruturados em Cluster a fim de manter a funcionalidade de alta disponibilidade do serviço arquivos em rede na Secretaria de Estado da Saúde (SES S. Paulo).

7.7.3.Servidores de rack do Cluster de Oracle

Estes ativos são responsáveis pela solução de banco de dados Oracle em cluster a fim de manter a funcionalidade de alta disponibilidade do serviço de banco na Secretaria de Estado da Saúde (SES S. Paulo).

7.7.4.Servidor Failover Active Directory

Este ativo é um dos servidores de failover do Active Directory, na possível falha dos outros servidores virtuais com a mesma role no Datacenter Secretaria de Estado da Saúde (SES S. Paulo).

7.7.5.Servidor DHCP

Este ativo é um servidor de DHCP, responsável pela entrega de IP dos desktops da rede interna da Secretaria de Estado da Saúde (SES S. Paulo) dos prédios Arnaldo e Eneas.

7.7.6.Servidor Serviço Tableau

Este ativo é um servidor do serviço Tableau responsável por dashboards de dados e projetos da Secretaria de Estado da Saúde (SES S. Paulo) publicados para o cidadão.

7.7.7.Servidor VMware Vcenter Server Appliance

Este ativo é um servidor em forma de appliance virtual para gerenciamento do cluster de host de ESXi da VMware.

7.7.8.Servidor Sistema SANI

Este ativo é um servidor do Sistema SANI, responsável pelos pagamentos de serviços prestados da Secretaria de Estado da Saúde (SES S. Paulo) de terceiros.

7.7.9.Servidor Projeto COVID

Estes ativos são servidores parte integrada do projeto COVID para o processamento de carga de testes de COVID.

7.7.10.Servidor de Repositório de backup

Este ativo é um servidor responsável pela função de proxy para o repositório de backup em disco da solução de backup do Datacenter da Secretaria de Estado da Saúde (SES S. Paulo).

7.7.11.Servidor de logs Firewall Watchguard

Este ativo é um servidor responsável pela função de armazenamento de logs de acesso do firewall Watchguard no Datacenter da Secretaria de Estado da Saúde (SES S. Paulo).

7.7.12.Solução de switch Brocade

Os switches Brocade permitem a comunicação entre vários servidores e dispositivos de armazenamento oferecendo múltiplos caminhos disponíveis para o transporte de dados entre 2 (dois) pontos, utilizando o protocolo Fibre Channel (FCP).

7.7.13.Sala cofre / Data Center

Os ativos relacionados neste item compõem a infraestrutura física (rack, servidores, ar-condicionado, piso elevado, nobreak, porta corta-fogo e CFTV) que compõem itens essenciais básicos para o funcionamento do Datacenter da Secretaria de Estado da Saúde (SES S. Paulo).

7.8.Software Licenciamento

Atualmente, as informações de licenciamento são de propriedade da Secretaria de Estado da Saúde (SES S. Paulo), que faz aquisição direta com informações de

vigências de contrato que permitam o suporte direto do fabricante para correções de falhas, atualizações e outras funcionalidades.

7.9.DNS

O DNS saúde, está hospedado no Datacenter da Secretaria de Estado da Saúde (SES S. Paulo), (Marte) e Datacenter Prodesp (PAYSANDU), sendo de responsabilidade do publicador de Domínio sp.gov.br (https://www.dominio.sp.gov.br) onde ele aponta para os servidores Marte (master) e Paysandu (redundante) a tarefa de resolução de nomes.

7.10.Ambientes de apoio operacional (CVS e IAL)

7.10.1.CVS

A Vigilância Sanitária TI - CVS está situada no mesmo prédio que o Data Center da Secretaria de Estado da Saúde (SES S. Paulo), que dá apoio operacional de TI para o mesmo para continuidade de serviço da CVS.

Como a operação Data Center Secretaria de Estado da Saúde (SES S. Paulo), tem por finalidade o apoio a TI – CVS na continuidade de serviço, quaisquer tipos de falhas de hardware ou licenças não são de administração do Data Center Secretaria de Estado da Saúde (SES S. Paulo).

7.10.2.IAL

A equipe responsável pela TI do IAL está situada no mesmo quadrilátero que o Data Center Secretaria de Estado da Saúde (SES S. Paulo), que dá apoio operacional de TI para o mesmo para continuidade de serviço do IAL. Como a operação Data Center Secretaria de Estado da Saúde (SES S. Paulo), tem por finalidade o apoio a TI – IAL na continuidade de serviço, quaisquer tipos de falhas

de hardware ou licenças não são de administração do Data Center Secretaria de Estado da Saúde (SES S. Paulo).

7.11.Equipe de suporte e apoio a TIC da SESSP

Atualmente o Data Center Secretaria de Estado da Saúde (SES S. Paulo), possui uma equipe para de execução de SERVIÇOS e PROJETOS de apoio de informática às áreas estratégias do negócio.

Nessa equipe a gestão das atividades dos profissionais é de responsabilidade da contratante.

8. SUGESTÕES DE MELHORIAS FUTURAS

Sugestão de novos relatórios de análise:

- Identificar Ativos
- Identificar Possíveis Riscos
- Elaborar Questionários
- Responder Questionários
- Consolidar Questionários
- Mensurar Riscos Identificados
- Elaborar Relatórios de Análise
- Definir Critérios de Tratamento
- Elaborar Plano de Tratamento
- Tratar Riscos
- Elaborar Relatório de Execução
- Revisar Processo

Identificar Ativos		
Descrição	Identifica os ativos e seus componentes.	
Considerações Importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Inventário de Ativos.	
Saídas	Rol de ativos, componentes e responsáveis.	
Atividades	**Consultar Inventário de Ativos**	Obtém informações dos ativos e seus componentes, consultando o Inventário de Ativos.
	Registro Ativos do Escopo	Armazenar adequadamente o rol de ativos e seus componentes, bem como os seus responsáveis.

Identificar Possíveis Riscos		
Descrição	Para cada ativo e seus componentes, identifica os possíveis riscos associados.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Rol de ativos, componentes e responsáveis.	
Saídas	Rol de possíveis riscos e controles associados para cada ativo e seus componentes.	
Atividades	**Consultar Base de Conhecimento**	Consultar base de conhecimento para levantar os possíveis riscos de cada ativo e seus componentes,bem como os possíveis controles que possam minimizar os riscos.
	Registrar Possíveis Riscos	Armazenar adequadamente os possíveis riscos de cada ativo e seus componentes e seus controles associados.

Elaborar Questionários		
Descrição	Elaborar os questionários para identificação dos riscos dos ativos e seus componentes.	
Considerações importantes	Caso seja possível, será realizada coleta automática de informações dos riscos dos ativos e seus componentes.	
Papéis	Unidade de SI.	
Entradas	Rol de ativos, componentes e responsáveis; rol de possíveis riscos e controles associados para cada ativo e seus componentes.	
Saídas	Questionário de identificação de riscos.	
Atividades	**Elaborar Questionário**	Para cada ativo e componente, consolidar as entradas acima para compor questionário visando identificar quais os controles foram implementados ou não.
	Coletar Informações Automaticamente	Caso possível, fazer coleta automática de informações de riscos, completando o que for possível nos questionários de identificação de riscos.
	Disponibilizar Questionários	Disponibilizar os questionários de identificação de riscos para os responsáveis pelos ativos e definir prazo para resposta e devolução dos mesmos.

Responder Questionários		
Descrição	Responder questionário de identificação de riscos.	
Considerações importantes	N/A	
Papéis	Unidade Responsável Pelo Ativo	
Entradas	Questionário de identificação de riscos para cada ativo de sua responsabilidade.	
Saídas	Questionário de identificação de riscos respondido para cada ativo do escopo do processo.	
Atividades	**Verificar Controles**	Para cada ativo e seus componentes, verificar quais os controles estão implementados ou não.
	Preencher Questionário	Com base nas informações obtidas na atividade anterior,preencher o questionário de identificação de riscos.
	Devolver Questionário Respondidos	Devolver para a Unidade de SI os questionários respondidos no prazo estabelecido.

Consolidar Questionários		
Descrição	Consolidar os questionários de identificação de riscos respondidos.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos respondidos.	
Saídas	Consolidação de todos os questionários de identificação de riscos respondidos.	
Atividades	**Registrar Questionários**	Armazenar adequadamente os questionários de identificação de riscos respondidos.

Mensurar Riscos Identificados		
Descrição	Com base nos questionários de identificação de riscos respondidos, calcular o risco para cada ativo, componente e do escopo.	
Considerações importantes	O Índice de Risco será calculado de acordo com a metodologia adotada pela ferramenta que auxilia o processo e será dado em percentual.	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos consolidados.	
Saídas	Índices de Risco de cada ativo, componente e do escopo do processo.	
Atividades	**Calcular Índices de Risco**	Para cada ativo, componente e o escopo inteiro, calcular o Índice de Risco.
	Registrar Índices de Risco	Armazenar adequadamente os Índices de Risco calculados.

Elaborar Relatórios de Análise		
Descrição	Elaborar Relatório de Análise de Riscos e Relatório Operacional de Riscos.	
Considerações importantes	Os relatórios seguirão modelo da ferramenta que auxilia o processo.	
Papéis	Unidade de SI.	
Entradas	Questionários de identificação de riscos consolidados e Índices de Risco de cada ativo, componente e do escopo do processo.	
Saídas	Relatório de Análise de Riscos e Relatório Operacional de Riscos.	
Atividades	**Confeccionar Relatórios**	Com base nas informações obtidas nas entradas acima, fazer o Relatório de Análise de Riscos e o Relatório Operacional de Riscos.
	Registrar Relatórios	Armazenar os relatórios de maneira adequada.
	Encaminhar Relatórios	Encaminhar os relatórios acima para apreciação do Comitê Gestor de Segurança da Informação.

Avaliar Ciclo		
Descrição	Avaliar a cadeia de valor do Processo de Gestão de Riscos.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Execução de Plano de Tratamento de Riscos.	
Saídas	Relatório de Execução de Plano de Tratamento de Riscos revisado.	
Atividades	**Discutir Relatório**	Discutir resultados apresentados no Relatório de Execução do Plano de Tratamento de Riscos.
	Definir melhorias	Definir melhorias para o Processo de Gestão de Riscos de Segurança da Informação.

Definir Critérios de Tratamento		
Descrição	Definir os critérios de tratamento de riscos que selecionarão os controles que deverão ser implementados.	
Considerações importantes	Os controles que não forem abrangidos pelos critérios de tratamento de riscos terão os riscos da sua não implementação aceitos.	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Análise de Riscos e o Relatório Operacional de Riscos.	
Saídas	Critérios de tratamento de riscos.	
Atividades	**Discutir o que Tratar**	Debater sobre quais riscos a instituição deve tratar.
	Estabelecer Critério	Definir o que tratar. Por exemplo: Riscos Muito Altos

Elaborar Plano de Tratamento		
Descrição	Elaborar Plano de Tratamento de Riscos de acordo com os critérios estabelecidos pelo CGSI.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Relatório Operacional de Riscos e critérios de tratamento de riscos.	
Saídas	Plano de Tratamento de Riscos.	
Atividades	**Elaborar Plano**	Considerando os critérios de tratamento de riscos estabelecidos pelo CGSI, elaborar o Plano de Tratamento de Riscos baseado no subconjunto do ROR.
	Disponibilizar Plano	Disponibilizar Plano de Tratamento de Riscos para as unidades responsáveis pelos ativos e estabelecer prazo.

Tratar Riscos		
Descrição	Tratar os riscos dos ativos sob a sua responsabilidade.	
Considerações importantes	N/A	
Papéis	Unidade Responsável pelo Ativo.	
Entradas	Plano de Tratamento de Riscos.	
Saídas	Plano de Tratamento de Riscos atualizado.	
Atividades	**Implementar Controle**	Quando viável, implementar os controles propostos no Plano de Tratamento de Risco.
	Documentar Implantação	Armazenar adequadamente os procedimentos adotados na implantação dos controles propostos no Plano de Tratamento de Riscos. Indicar no Plano de Tratamento de Riscos que o controle foi implementado.
	Justificar não Implementação	Quando não for viável a implantação de um controle, registrar no Plano de Tratamento de Riscos a justificativa.
	Devolver o PTR atualizado	Devolver o PTR atualizado para a Unidade de Segurança da Informação.

Elaborar Relatório de Execução		
Descrição	Elaborar Relatório de Execução do Plano de Tratamento de Riscos.	
Considerações importantes	N/A	
Papéis	Unidade de SI.	
Entradas	Relatório de Análise de Riscos, Relatório Operacional de Riscos, Plano deTratamento de Riscos, Critérios de Tratamento de Risco.	
Saídas	Relatório de Execução de Plano de Tratamento de Riscos.	
Atividades	**Calcular Indicadores**	Calcular os indicadores do processo, de acordo com item10.
	Elaborar Relatório	Elaborar relatório resumido do ciclo do processo, indicando os fatos relevantes, os indicadores, evolução do risco e sugestões de melhoria.

Avaliar Cadeia de Valor		
Descrição	Avaliar Cadeia de valor do Processo de Gestão de Riscos.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Execução de Plano de Tratamento de Riscos.	
Saídas	Relatório de Execução de Plano de Tratamento de Riscos revisado.	
Atividades	**Discutir Relatório**	Discutir resultados apresentados no Relatório de Execução do Plano de Tratamento de Riscos.
	Definir melhorias	Definir melhorias para o Processo de Gestão de Riscosde Segurança da Informação.

Revisar Processo		
Descrição	Revisar o Processo de Gestão de Riscos de Segurança da Informação.	
Considerações importantes	N/A	
Papéis	Comitê Gestor de Segurança da Informação.	
Entradas	Relatório de Execução de Plano de Tratamento de Riscos revisado.	
Saídas	Processo de Gestão de Riscos de Segurança da Informação revisado.	
Atividades	**Fazer Análise Crítica do Processo**	Avaliar se o processo está atendendo as necessidades da instituição.
	Definir Melhorias	Definir melhorias a serem adotadas no processo.

9. INDICADORES DE DESEMPENHO

9.1.Nível de Risco de Segurança da Informação

Indicador 1	
Objetivo	Avaliar o Nível de Risco de Segurança da Informação da instituição.
Indicador	Percentual de Risco de Segurança da Informação após o tratamento dos riscos.
Responsável pelamedição	Unidade de SI.
Período de Medição	Anual.

9.2.Eficiência do Processo

Indicador 2	
Objetivo	Avaliar a eficiência do Processo de Gestão de Riscos de Segurança da Informação
Indicador	(Nível de Risco de Segurança da Informação antes do tratamento menos o Nível de Risco de Segurança da Informação após o tratamento) / Nível de Risco de Segurança da Informação antes do tratamento.
Responsável pelamedição	Unidade de SI.
Período de Medição	Anual.

9.3.Eficácia do Processo

Indicador 3	
Objetivo	Avaliar a eficácia do Processo de Gestão de Riscos de Segurança da Informação
Indicador	1 – Se o Nível de Risco de Segurança da Informação após o tratamento estiver dentro da meta de risco aceitável (apetite de risco) da instituição. 0 – Caso contrário.
Responsável pelamedição	Unidade de SI.
Período de Medição	Anual.

10. Histórico de Versões

Data de atualização	Versão	Procedimento	O que foi feito	Alterações Realizadas	Item
25/11/2022	1.0	**10**	Incluído histórico de Versões	Inclusão	N/A
25/11/2022	1.0	**N/A**	Alterado Liderança	Retirado Kathya Esteves, mantido Janilton Santana	N/A
02/03/2023	1.0	**N/A**	Alteração Liderança	Atualização Liderança	N/A

11. Referências

ITIL 4

Glossário ITIL 4

Glossário-ITIL-4-Fnd-português-v122 Pages 1-50 - Flip PDF Download | FlipHTML5