

Secretaria de TIC do TRT24

Processo Gerenciar Incidentes de Segurança da Informação

HISTÓRICO DO DOCUMENTO

	DATA	DESCRIÇÃO
01	07/12/2015	Desenho do processo
02	26/04/2016	Descrição do processo
03	23/09/2016	Revisão do desenho e alinhamento COBIT 5.0
04	23/08/2018	Alinhamento à nova versão da Política de Segurança da Informação
05	30/06/2022	Revisão do desenho e do fluxo das atividades do processo
06	04/03/2024	Revisão do processo

Secretaria de TIC do TRT da 24ª Região
Documento de Descrição de Processo de Trabalho
Processo Gerenciar Incidentes de Segurança da Informação

04/03/2024

EQUIPE DE DOCUMENTAÇÃO

	Nome	Cargo
01	João Carlos Ferreira Filho	Chefe da Divisão de Governança de TIC
02	Geslaine Perez Maquerte	Chefe da Divisão de Proteção de Dados e Segurança da Informação
03	Alex Sandro Pontes da Silva	Chefe do Setor de Apoio a Processos e Iniciativas Nacionais

Sumário

1	OBJETIVOS	4
2	ABRANGÊNCIA	4
3	DEFINIÇÕES	4
4	PROCESSO GERENCIAR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	5
4.1	PAPÉIS E RESPONSABILIDADES	5
4.2	FLUXO DO PROCESSO	6
4.3	DESCRIÇÃO DO PROCESSO	7
5	TABELA RACI	11
6	MÉTRICAS DO PROCESSO	12
6.1	DESCRIÇÃO DA MÉTRICA	12
7	DIVULGAÇÃO DOS RESULTADOS	12
8	ANEXO I – MÉTRICA NÚMERO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	13
9	ANEXO II – ESCALA DE RELEVÂNCIAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	14
10	ANEXO III – ESCALA DE SEVERIDADES DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	14
11	ANEXO IV – MATRIZES DE CLASSIFICAÇÃO DE IMPACTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	15

1 OBJETIVOS

Gerenciar os incidentes de segurança da informação do TRT da 24ª Região.

2 ABRANGÊNCIA

Secretaria de Tecnologia de Informação e Comunicações.

3 DEFINIÇÕES

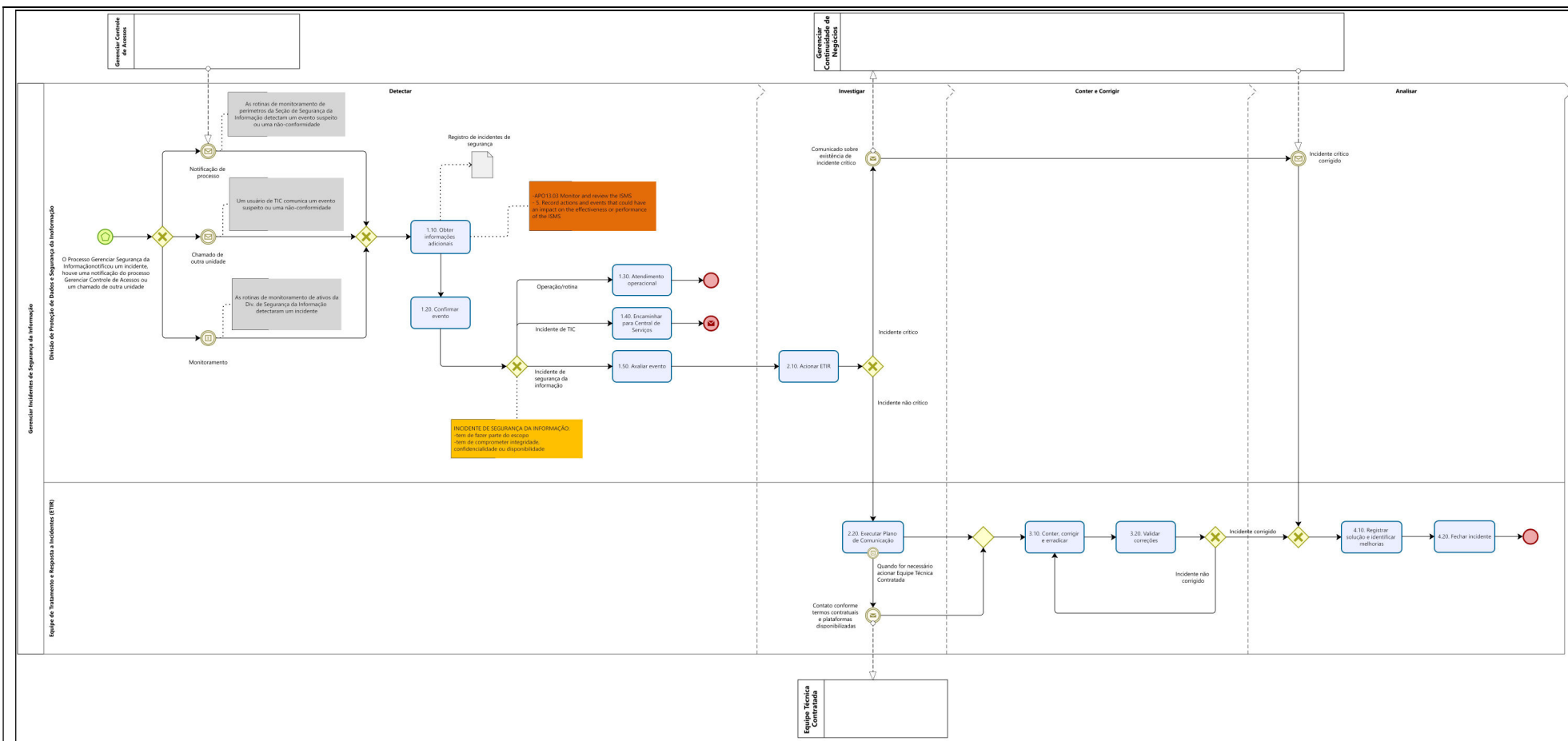
- **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do TRT24;
- **Ativos de TIC:** qualquer mecanismo ou dispositivo de software ou hardware que compõem a infraestrutura da rede de dados do TRT24 e que é utilizado como ferramenta de trabalho para o desempenho funcional dos magistrados e servidores do Tribunal;
- **Base de conhecimentos:** conjunto de conhecimentos acumulados a respeito dos incidentes e seus respectivos tratamentos;
- **ETIR:** Equipe de tratamento e resposta a incidentes
- **Ferramenta ITSM:** Aplicação utilizada para o gerenciamento de serviços de TIC
- **Incidente de segurança da informação:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade. São exemplos de incidentes de segurança da informação:
 - a. perda de serviço, equipamentos ou recursos;
 - b. mau funcionamento ou sobrecarga de sistema;
 - c. erros humanos;
 - d. não-conformidade com políticas ou diretrizes;
 - e. violação de procedimentos de segurança física;
 - f. mudanças descontroladas de sistemas;
 - g. mau funcionamento de software ou hardware;
 - h. violação de acesso;
- **Usuário de TIC:** todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em qualquer unidade organizacional do TRT da 24ª Região.

4 Processo Gerenciar Incidentes de Segurança da Informação

4.1 Papéis e Responsabilidades

Papel	Responsabilidades	Responsável
Dono do Processo	● Buscar a qualidade e eficiência gerais do processo ● Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados ● Aprovar as atualizações do processo.	Secretário de Tecnologia da Informação e Comunicações
Gerente do Processo	● Buscar a eficiência e a efetividade do processo ● Produzir informações gerenciais (indicadores) ● Promover a execução das atividades do processo ● Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Divisão de Proteção de Dados e Segurança da Informação	● Executar as atividades do Processo Gerenciar Incidentes de Segurança da Informação.	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Equipe de Tratamento e Resposta à Incidente	● Executar as ações necessárias e pertinentes para tratar o incidente de segurança da informação ● Validar as correções com as áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade ● Descrever a solução do incidente e registrar as eventuais melhorias que podem ser implantadas para evitar ou mitigar a repetição do mesmo tipo de incidente ● Registrar o fechamento do incidente	Servidores indicados pelo Gerente do Processo para atuarem no tratamento do incidente
Equipe Técnica Contratada	● Executar atividades do processo externo denominado “Equipe técnica contratada”	Fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem

4.2 Fluxo do Processo



4.3 Descrição do Processo

Id	Atividade	Responsável	Descrição
1.10	Obter informações adicionais	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: Evento detectado
			Processamento: - Obter o maior número possível de informações sobre o evento: nome e unidade do usuário comunicador; dia e hora que o evento ocorreu; como foi detectado o incidente; quais operações estão indisponíveis; que sistemas foram afetados; etc. - Anotar as informações em ferramenta de registro de incidentes, contendo pelo menos as possibilidades de pesquisa dos incidentes de segurança para manutenção de base de lições aprendidas nos registros. Observação: No registro realizado o incidente deve ser mantido com status “aberto”, ainda que contendo subchamados para atendimento emergencial e solucionador até a finalização completa das medidas de sanitização (primárias e secundárias).
			Saídas: Preenchimento de todos os dados em ferramenta de registro de incidentes.
1.20	Confirmar evento	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: Registro de Incidente de Segurança da Informação
			Processamento: - Confirmar se o evento realmente configura um incidente de segurança da informação. - Preencher o tipo de incidente adequadamente “incidente operacional” ou “incidente de segurança da informação”, na ferramenta utilizada.
			Saídas: Tipo do incidente consolidado corretamente na ferramenta de Registro de Incidentes de Segurança da Informação.
			Caso o incidente seja do tipo operacional/rotina , seguir para “Realizar atendimento operacional”
			Caso o incidente seja do tipo incidente de TIC , seguir para “Encaminhar para Central de Serviços”
			Caso o incidente seja do tipo incidente de segurança da informação , seguir para “Avaliar evento”
1.30	Realizar atendimento operacional	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entrada: Informações relativas ao incidente
			Processamento: Executar a operação/rotina necessária para a solução do incidente
			Saída: Incidente solucionado
1.40	Encaminhar para Central de Serviços	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: Registro de Incidente de TIC
			Processamento: Cadastrar ou atualizar incidente na ferramenta ITSM de uso pela Central de Serviços

Secretaria de TIC do TRT da 24ª Região
Documento de Descrição de Processo de Trabalho
Processo Gerenciar Incidentes de Segurança da Informação

04/03/2024

Id	Atividade	Responsável	Descrição
			Saídas: Cadastramento ou atualização na ferramenta ITSM.
1.50	Avaliar evento	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: Registro de Incidentes de Segurança da Informação Processamento: • Descrever e avaliar os reais impactos do incidente de segurança da informação. Lançar nota na ferramenta de registro indicando o impacto do incidente, utilizando os valores das tabelas de classificação dos ANEXOS II e III e a matriz do ANEXO IV: ○ É considerado incidente crítico aquele cujo impacto indicado é alto ou muito alto ○ É considerado incidente não crítico aquele cujo impacto indicado é baixo ou médio • Registrar o incidente como em investigação, e estimar o tempo necessário para investigação, contenção e correção do incidente. As seguintes informações serão necessárias para as lições aprendidas e podem ser anotadas durante cada etapa de registro para evitar perda de informações: a) A identificação e análise da causa-raiz do incidente; b) A linha do tempo das ações realizadas; c) A escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise; d) Os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas; e) O escalonamento da crise; f) A investigação e preservação de evidências; g) A efetividade das ações de contenção; h) A coordenação da crise, liderança das equipes e gerenciamento de informações; e i) A tomada de decisão e as estratégias de recuperação. Saídas: Preenchimento das informações iniciais de impacto e tempo de resposta estimado na ferramenta de registro.
2.10	Acionar ETIR	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: Registro de Incidente de Segurança da Informação Processamento: • Acionar a equipe que tratará o incidente de segurança da informação, conforme atribuições de cada unidade pertencente à ETIR - definida pela Política de Gestão de Incidentes de Segurança da Informação. • Abrir subchamados na ferramenta para cada serviço sob responsabilidade dos integrantes da ETIR. Saídas: Abertura de subchamados para os integrantes da ETIR para o Incidentes de Segurança da Informação

Secretaria de TIC do TRT da 24ª Região
Documento de Descrição de Processo de Trabalho
Processo Gerenciar Incidentes de Segurança da Informação

04/03/2024

Id	Atividade	Responsável	Descrição
			No caso de incidente crítico , seguir para comunicar o processo Gerenciar Continuidade de Negócios sobre a existência de incidente crítico
			No caso de incidente não crítico , seguir para “Executar Plano de Comunicação”
2.20	Executar Plano de Comunicação	Equipe de Tratamento e Resposta à Incidente	Entradas: Registro de Incidente de Segurança da Informação
			Processamento: - Comunicar incidente às áreas afetadas e envolvidas, através da comunicação entre os integrantes da ETIR e o proprietário do ativo de TIC - Comunicar a Central de Serviços para que seja feita a triagem dos eventuais chamados relacionados ao incidente em questão - Quando a execução dos procedimentos para tratamento do incidente envolver fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem, acionar a Equipe Técnica Contratada nos termos contratuais e plataformas disponibilizadas, podendo haver acionamento direto pelos integrantes da ETIR com os contatos disponibilizados pelos contratados
			Saídas: Comunicados enviados
3.10	Conter, corrigir e erradicar	Equipe de Tratamento e Resposta à Incidente	Entradas: informações do Registro de Incidentes de Segurança da Informação
			Processamento: - Abrir subchamados para tratamentos distintos pelas diferentes equipes internas da SETIC. - Atividades executadas dentro da SPDSEG, registrar dentro do chamado principal. - Executar as ações necessárias e pertinentes para tratar o incidente de segurança da informação. - Registrar todas as tratativas realizadas dentro dos chamados e subchamados.
			Saídas: Abertura de subchamados para cada tratamento realizado (emergencial ou definitivo) ou para cada serviço afetado e atendido por diferentes integrantes da ETIR ou equipes internas e preenchimento dos tratamentos a serem realizados.
3.20	Validar correções	Equipe de Tratamento e Resposta à Incidente	Entradas: Informações do Registro de Incidentes de Segurança da Informação e informação sobre a solução do incidente
			Processamento: Validar as correções com as áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade
			Saídas: Aceite (confirmação) das áreas afetadas

Secretaria de TIC do TRT da 24ª Região
Documento de Descrição de Processo de Trabalho
Processo Gerenciar Incidentes de Segurança da Informação

04/03/2024

Id	Atividade	Responsável	Descrição
			Caso o incidente tenha sido corrigido, seguir para “Registrar solução e identificar melhorias” Caso o incidente não tenha sido corrigido, seguir para “Conter, corrigir e erradicar”
4.10	Registrar solução e identificar melhorias	Equipe de Tratamento e Resposta à Incidente	Entradas: Registro de Incidente de Segurança da Informação e informação sobre a solução do incidente Processamento: • Descrever a solução do incidente e registrar as eventuais melhorias que podem ser implantadas para evitar ou mitigar a repetição do mesmo tipo de incidente. As seguintes informações serão necessárias para as lições aprendidas e podem ser anotadas durante cada etapa de registro para evitar perda de informações: a) A identificação e análise da causa-raiz do incidente; b) A linha do tempo das ações realizadas; c) A escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise; d) Os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas; e) O escalonamento da crise; f) A investigação e preservação de evidências; g) A efetividade das ações de contenção; h) A coordenação da crise, liderança das equipes e gerenciamento de informações; e i) A tomada de decisão e as estratégias de recuperação. • Abrir chamados de melhorias relacionados ao incidente de segurança da informação para pesquisa posterior, ou, quando for o caso, enviar demanda de ação ou projeto para o Secretário de TIC. Saídas: Preenchimento de dados em ferramenta de Registro de Incidentes de Segurança da Informação
4.20	Fechar incidente	Equipe de Tratamento e Resposta à Incidente	Entradas: Registro de Incidente de Segurança da Informação Processamento: • Registrar o fechamento do incidente. Saídas: Registro do incidente de segurança da informação na ferramenta como “fechado”.

5 Tabela RACI

	Atividade	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Equipe de Tratamento e Resposta à Incidente
1.10	Obter informações adicionais	R	
1.20	Confirmar evento	R	
1.30	Realizar atendimento operacional	R	
1.40	Encaminhar para Central de Serviços	R	
1.50	Avaliar evento	R	
2.10	Acionar ETIR	R	
2.20	Executar Plano de Comunicação		R
3.10	Conter, corrigir e erradicar		R
3.20	Validar correções	C	R
4.10	Registrar solução e identificar melhorias		R
4.20	Fechar incidente		R

Legenda: Responsável (R), Consultado (C), Informado (I)

6 Métricas do processo

6.1 Descrição da métrica

Nome da métrica	Número de incidentes de Segurança da Informação
Origem	Controle elaboração pela Divisão de Proteção de Dados e Segurança da Informação
Objetivo	Quantificar a quantidade de ocorrências de incidentes registradas e tratadas conforme o processo
Periodicidade	Trimestral
Forma de cálculo	Contagem da quantidade de incidentes de segurança registrados na ferramenta de gestão durante o período de apuração
Fonte	- Planilha do ANEXO I Total de incidentes: soma do total de linhas referentes ao período de apuração

7 Divulgação dos Resultados

Os resultados do processo serão demonstrados através dos indicadores de desempenho disponibilizados no site de governança de TIC da Secretaria de Tecnologia da Informação e Comunicações, menu Indicadores, item Indicadores de Processos, processo Gerenciar Incidentes de Segurança da Informação.

8 ANEXO I – Métrica Número de Incidentes de Segurança da Informação

Data do incidente	Tipo	Descrição do incidente

Onde:

- Para cada incidente:
 - **Data do incidente:** data da ocorrência;
 - **Tipo:** Incidente crítico ou incidente não crítico
 - **Descrição do incidente:** breve descrição para fins de identificação da ocorrência

9 ANEXO II – Escala de Relevâncias de Incidentes de Segurança da Informação²

Descritor	Descrição	Nível
Muito baixa	Afeta uma parte muito pequena e localizada do negócio da organização e os prejuízos são desprezíveis.	1
Baixa	Afeta uma parte pequena e localizada do negócio da organização e os prejuízos são baixos.	2
Média	Afeta uma parte do negócio da organização e os prejuízos são razoáveis.	3
Alta	Afeta um ou mais negócios da organização e os prejuízos são muito altos.	4
Muito Alta	Afeta toda a organização e os prejuízos são extremamente altos.	5

10 ANEXO III – Escala de Severidades de Incidentes de Segurança da Informação

Descritor	Descrição	Nível
Muito baixo	Degradação do negócio da organização, porém afetando minimamente os objetivos (prazo, custo, qualidade, escopo, imagem, etc.) relacionados a metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação do negócio da organização, afetando pouco os objetivos.	2
Médio	Interrupção no negócio da organização, afetando significativamente os objetivos, porém passível de recuperação.	3
Alto	Interrupção no negócio da organização, causando danos de reversão muito difícil nos objetivos.	4
Muito Alto	Paralisação no negócio da organização, causando danos irreversíveis nos objetivos.	5

² Instruções de uso:

1º) Classifique o incidente de segurança da informação quanto a sua relevância, usando as descrições do Anexo II;

2º) Classifique o incidente de segurança da informação quanto a sua severidade, usando as descrições do Anexo III;

3º) Determine o impacto do incidente de segurança da informação, fazendo o cruzamento dos valores obtidos nos passos 1º e 2º na Matriz de Classificação de Impacto de Incidentes de Segurança da Informação (Anexo IV).

11 ANEXO IV – Matrizes de Classificação de Impacto de Incidentes de Segurança da Informação

Matriz de Classificação de Impacto

		Severidade				
		1 Muito baixa	2 Baixa	3 Média	4 Alta	5 Muito alta
Relevância	5 Muito Alta	5	10	15	20	25
	4 Alta	4	8	12	16	20
	3 Média	3	6	9	12	15
	2 Baixa	2	4	6	8	10
	1 Muito Baixa	1	2	3	4	5

Classificação dos impactos:

Baixo

Médio

Alto

Muito Alto