Processo de Gestão de Incidentes de Segurança da Informação

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TRT-14ª REGIÃO
Rondônia e Acre

JOENIR JOSE DELLA FLORA
18/06/2024 13:46

WAINNER BRUM CAETANO
20/06/2024 08:08

Gestor do Processo: Chefe da Divisão de Segurança da Informação
Área responsável: Divisão de Segurança da Informação - SETIC

OBJETIVO

Estabelecer o Processo de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 14º Região (TRT14), definindo papéis e responsabilidades, procedimentos a serem adotados no tratamento de incidentes de segurança da informação e detalhes de comunicação.

DEFINIÇÕES GERAIS PARA A ADEQUADA EXECUÇÃO DESTE PROCESSO

Regras Gerais

O processo será coordenado pela “Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação” (ETIR), que é composta por servidores com a responsabilidade de detectar, receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação. Todos que fazem parte da ETIR devem atuar diretamente em todas as ações realizadas;

A ETIR deve ser notificada o mais rápido possível de quaisquer eventos ou incidentes de segurança da informação no âmbito do TRT14;

A ETIR tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas;

Os incidentes de segurança da informação podem ser notificados por qualquer usuário de TIC do TRT14, ou informados por equipes de tratamento e resposta a incidentes de segurança pertencentes a organizações externas ao TRT14.

Todas as informações e ações para tratamento de incidentes de segurança da informação devem ser registradas no RISI - Relatório de Incidente de Segurança da Informação.

Tipificação dos Incidentes de Segurança da Informação

Os eventos ou incidentes de segurança da informação que serão tratados pela ETIR incluem, mas não estão limitados a:

- Violação da Política de Segurança da Informação do TRT14;
- Ocorrência de execução de malware;
- Comprometimento de credenciais;
- Identificação de vulnerabilidade;
- Ocorrência de Intrusão/ataque;
- Discussão de assuntos sigilosos em ambientes públicos;
- Violação de informações sensíveis (confidencial ou restrita);
- Violação de Dados Pessoais (LGPD).

Monitoramento e Detecção dos Incidentes de Segurança

O monitoramento do ambiente interno deve identificar vulnerabilidades, alvos de ataques em curso e sistemas comprometidos, bem como sugerir medidas preventivas e corretivas. As atividades de monitoramento devem incluir, conforme a disponibilidade de recursos para a ETIR:

- Monitoramento, por amostragem e em tempo real, do comportamento da rede, estações e servidores, por meio de logs e fluxos de rede;
- Acompanhamento das informações dos consoles de antivírus, firewalls, IPS, registros (logs) de rede;
- Identificação dos ataques em curso, por meio de desvios comportamentais dos sistemas e alertas.
- Identificação automatizada, registro e monitoramento das vulnerabilidades existentes.
- Adicionalmente, o monitoramento de incidentes de segurança da informação pode ser apoiado por meio de diversas fontes (listas de discussão, redes sociais, sites especializados, etc.).

Comunicação do Incidente de Segurança

A comunicação dos incidentes de segurança, comuns e rotineiros, será realizada por meio das reuniões da ETIR e de forma geral e resumida e por meio de relatórios e boletins.

Todas as informações detalhadas do incidente, incluindo todas as ações de todas as fases devem ser registradas no RISI.

Caso o incidente de segurança seja considerado penalmente relevante, será reportado por meio do sistema de processo administrativo de forma confidencial, pelo Chefe da Divisão de Segurança da Informação, ao responsável pela Segurança Institucional e a Presidência.

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e

deverá conter os itens constantes relacionados no Plano de Gestão de Incidentes de Segurança da Informação.

Papéis e Responsabilidades

Papel		Responsabilidades
Presidência	Órgão diretivo do TRT	Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação.
Comitê de Segurança da Informação	Comitê multidisciplinar responsável pela coordenação das ações e deliberações relacionadas à área de segurança da TIC.	Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação.
Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação (ETIR)	Equipe responsável pelas atividades relacionadas ao tratamento e resposta a incidentes de segurança da informação	Monitorar o ambiente e recursos de TIC do TRT, a fim de identificar possíveis incidentes de segurança da informação. Realizar a investigação do incidente de segurança da informação, propondo medidas de contenção. Assessorar o Comitê de Segurança da Informação e a SETIC na análise e tomada de decisões a respeito de situações resultantes de incidentes de segurança da informação. Realizar a análise do incidente de segurança da informação, de forma a propor medidas para eliminar ou solucionar problemas que causaram o incidente. Realizar a comunicação com o CTIR.BR.
Outras áreas da SETIC	Compreendem a Secretaria da SETIC, seus Núcleos, Seções e setores integrantes. Atuam em conjunto na análise e resolução dos incidentes quando acionados pela ETIR.	Auxiliar a ETIR na proposição e execução de medidas para contenção e solução de incidentes de segurança da informação. Autorizar, quando necessário, a execução das medidas propostas pela ETIR.

INTERFACE COM DEMAIS PROCESSOS

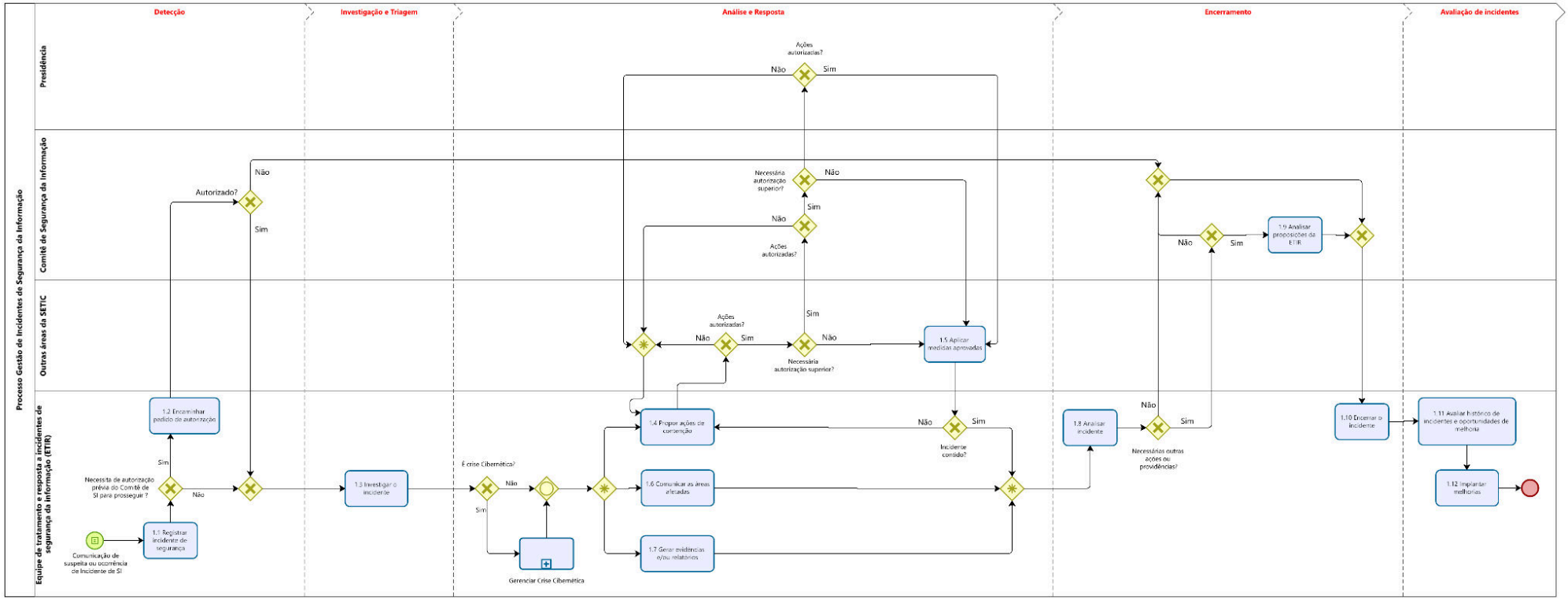
- **Gerenciamento de Configuração e Ativos de Serviço:** interação para assegurar que os ativos requeridos para a entrega de um serviço sejam adequadamente controlados, com informações seguras;
- **Gerenciamento de Eventos:** desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de

segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos;

- **Gerenciamento de incidentes de TIC:** o processo pode ser iniciado através de um incidente que já estava em tratamento no processo de gerenciamento de incidentes.
- **Subprocesso - Gerenciar Crise Cibernética:** o subprocesso será acionado quando o incidente se qualificar como Crise Cibernética, de acordo com as definições contidas na NSI04 - Gestão de Incidentes de Segurança da Informação.

FLUXOGRAMAS DESTE PROCESSO

Gerenciamento de Incidentes de Segurança da Informação

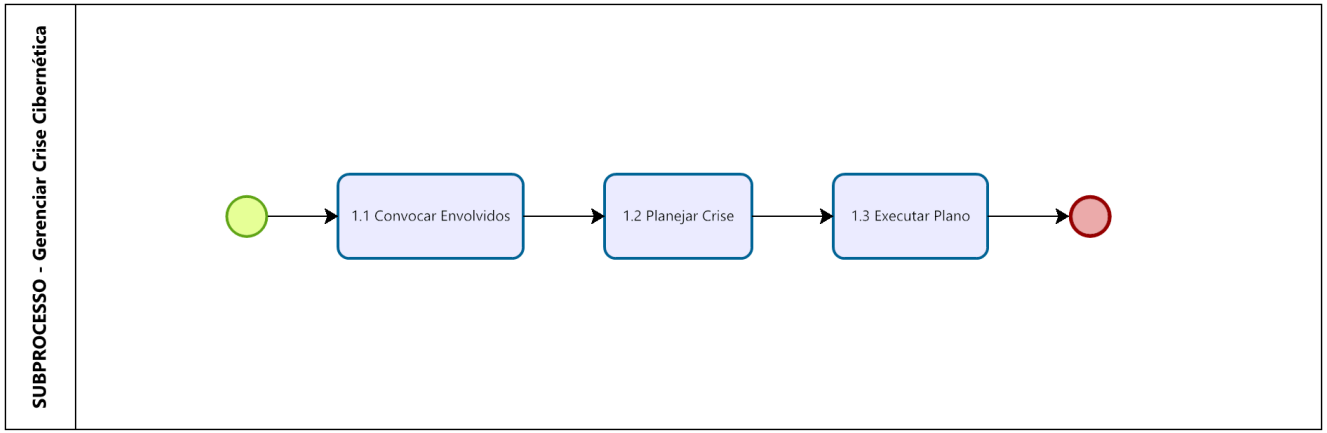


DESCRIÇÃO DAS ATIVIDADES DO FLUXOGRAMA			
Nome da atividade	**Objetivo**	**Responsável**	**Tarefas / Ações**
1.1 Registrar Incidente de Segurança	Detectar a ocorrência ou suspeita de ocorrência de incidente de segurança da informação, registrando-o de forma detalhada e categorizando-o.	ETIR	**Entrada:** Comunicação ou detecção de suspeita ou ocorrência de incidentes de Segurança da Informação. **Tarefas:** - Receber a comunicação sobre o incidente; - Detectar o incidente; - Solicitar esclarecimentos ao informante, quando necessário; - Registrar o incidente; - Verificar necessidade de autorização prévia do Comitê de Segurança da Informação. **Saída:** Formulário RISI preenchido com informações iniciais.
1.2 Encaminhar pedido de autorização	Solicitar autorização ao CSI para o prosseguimento da investigação nos casos em que há necessidade de emissão de relatórios de acesso de determinado(s) servidor(es) em sistemas e serviços disponibilizados, investigação de acessos não autorizados ou que exijam a verificação de dados dos usuários.	ETIR	**Entrada:** RISI – com registro de incidente que necessite de autorização. **Tarefas:** - Coletar as informações necessárias ao encaminhamento do pedido de autorização para prosseguimento da investigação; - Encaminhar pedido de autorização ao Comitê; - Prestar os esclarecimentos, quando necessário; - Encaminhar para investigação; - Encaminhar para finalização. **Saída:** Pedido de autorização ao Comitê de Segurança da Informação.
1.3 Investigar o incidente	A ETIR, com base nas informações inicialmente registradas no RISI, com o apoio das outras áreas, deverá investigar as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento.	ETIR	**Entrada:** Autorização do Comitê de Segurança da Informação e/ou RISI preenchido com as informações iniciais. **Tarefas:** - Verificar o tipo de incidente; - Analisar a extensão e o impacto causado pelo incidente; - Verificar se o tipo de incidente se caracteriza como Crise Cibernética. **Saída:** RISI preenchido com as informações do incidente investigado.

1.4 Propor ações de contenção	Propor ações para conter o incidente, que podem ser soluções de contorno ou de resolução do problema.	ETIR	**Entrada:** RISI preenchido com as informações sobre o incidente ou não aprovação das medidas anteriores ou informação de que as medidas não foram suficientes para conter o incidente. **Tarefas:** - Propor ações de contenção; - Encaminhar solução para aprovação das chefias; - Proposição de novas medidas, caso o incidente não seja contido; - Propor ações que visem gerenciar a crise cibernética, quando aplicável. **Saída:** RISI preenchido com as ações de contenção propostas.
1.5 Aplicar medidas aprovadas	Executar as ações propostas na fase anterior, visando conter o incidente, e verificar se o resultado esperado foi alcançado.	Outras áreas de TIC	**Entrada:** RISI com autorização da aplicação da medida de contenção proposta, quando necessária. **Tarefas:** - Aplicar as medidas necessárias; - Avaliar medidas aplicadas. **Saída:** RISI com resultados das medidas aplicadas.
1.6 Comunicar as áreas afetadas	Comunicar as áreas da SETIC sobre a ocorrência e, em conjunto com a Divisão de Segurança da Informação, deliberar se é necessário informar outras áreas do TRT sobre o incidente.	ETIR	**Entrada:** RISI preenchido com as informações sobre o incidente investigado. **Tarefas:** - Informar a extensão do impacto e quais sistemas/serviços foram afetados; - Definir como e a quem a comunicação será realizada; - Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados. **Saída:** Pedido à Direção da SETIC para comunicar áreas afetadas (se externo à SETIC) ou comunicação interna, com as informações necessárias + RISI preenchido com as informações sobre o plano de comunicação.
1.7 Gerar evidências e/ou relatórios	Dependendo do tipo de incidente, pode ser necessário a geração de evidências ou o relatório de logs de acesso.	ETIR	**Entrada:** RISI + Autorização do Comitê de Segurança da Informação. **Tarefas:** - Identificação dos dados necessários à elucidação do incidente; - Realizar a coleta e compilação de dados. **Saída:** Evidências ou Relatório de acessos.

1.8 Analisar incidente	Analisar o incidente como um todo (causa raiz identificada, ações de contenção aplicadas, resultados dos relatórios elaborados etc), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução).	ETIR	**Entrada:** RISI preenchido com todas as informações. **Tarefas:** - Analisar causa-raiz do incidente; - Propor melhorias no cenário investigado; -Redigir relatório; -Proposição de ações à Direção da SETIC. **Saída:** Solicitação de manifestação do Comitê de Segurança da Informação
1.9 Analisar proposições da ETIR	Avaliar as soluções propostas ou analisar o relatório de auditoria enviado pela ETIR, deliberando a respeito ou simplesmente tomando ciência acerca do incidente, quando for o caso.	Comitê de Segurança da Informação	**Entrada:** Proposição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). **Tarefas:** - Tomar ciência do incidente e medidas aplicadas; - Avaliar soluções propostas; - Analisar relatório de investigação/auditoria. **Saída:** Deliberação do Comitê de Segurança da Informação.
1.10 Encerrar o incidente	Nesta atividade, deve ser verificada a existência de providências ou determinações pendentes e providenciar sua execução.	ETIR	**Entrada:** Deliberação do Comitê de Segurança da Informação / RISI com providências. **Tarefas:** - Cumprir providências; - Encerrar o incidente; - Notificar o incidente ao CTIR.BR; - Notificar o incidente ao CPTRIC-PJ, em caso de incidente grave. **Saída:** RISI preenchido e encerrado / Notificação ao CTIR.BR (se necessário) / Notificação ao CPTRIC-PJ (se necessário).
1.11 Avaliar histórico de incidentes e oportunidades de melhoria	Analisar o tipo e histórico de incidentes, com o intuito de estudar o cenário "macro", de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de segurança da informação.	ETIR	**Entrada:** RISI encerrado. **Tarefas:** - Avaliar histórico de incidentes; - Alimentar indicadores estabelecidos; - Identificar oportunidades de melhoria. **Saída:** Registro de indicadores e proposta de ações de melhoria.
1.12 Implementar melhorias	Planejar e implementar as propostas de melhoria identificadas na atividade anterior.	ETIR	**Entrada:** Registro de indicadores e ações de melhoria. **Tarefas:** - Implantar melhorias e registrar lições aprendidas pós-crise quando aplicado. **Saída:** Melhorias implantadas.

SUBPROCESSO- Gerenciar Crise Cibernética



DESCRIÇÃO DAS ATIVIDADES DO FLUXOGRAMA			
Nome da atividade	**Objetivo**	**Responsável**	**Tarefas / Ações**
1.1 Convocar envolvidos	Convocar o Subcomitê de Crises Cibernéticas	ETIR	**Entrada:** Incidente classificado como Crise Cibernética. **Tarefas:** - Convocar o Subcomitê de Crises Cibernéticas; **Saída:** RISI preenchido com as informações do incidente investigado.
1.2 Planejar Crise	Definir um plano de atuação frente à Crise Cibernética.	ETIR/Subcomitê de Crises Cibernéticas	**Entrada:** RISI preenchido com as informações do incidente investigado. **Tarefas:** - entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos; - levantar todas as informações relevantes, verificando fatos e descartando boatos; - levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências; - avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

			- centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas; - realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas; - definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso; - aplicar os Protocolos da ENSEC-PJ que foram implantados; - avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar a ETIR; - orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz; - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e - elaborar plano de retorno à normalidade. - **Saída:** Plano de Resposta à Crise Cibernética.
1.3 Executar Plano	Executar as ações planejadas na fase anterior	ETIR/Subcomitê de Crises Cibernéticas	**Entrada:** Plano de Resposta à Crise Cibernética. **Tarefas:** - Colocar em execução as ações do Plano de Resposta à Crise Cibernética seguindo as atividades do processo de gerenciamento de incidentes de segurança da informação. **Saída:** Relatório das ações realizadas.

GLOSSÁRIO

Ação corretiva – Ação para eliminar a causa de um incidente identificado ou outra situação indesejável.

Ação preventiva – Ação para eliminar a causa de uma potencial não-conformidade ou outra situação potencialmente indesejável.

CPTRIC-PJ - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário.

Crise – Um evento ou série de eventos danosos que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

Crise Cibernética – decorre de incidentes em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

Evento de segurança da informação – Ocorrência identificada que pode afetar um ativo de informação associada a possível violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Evidência – Dados que apoiam a existência ou a veracidade de algo.

Malware – É um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

Incidente de segurança da informação - Ocorrência identificada e confirmada que afeta um ativo de informação com indicação de violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Integridade – Propriedade de salvaguarda da exatidão e completeza de ativos de informação.

Parte Interessada – Pessoa ou grupo que tem um interesse no desempenho ou no sucesso de uma organização.

RISI - Relatório de Incidente de Segurança da Informação

Vulnerabilidade – é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

REFERÊNCIAS

- Norma Complementar no 05/IN01/DSIC/GSIPR.
- Norma Complementar no 08/IN01/DSIC/GSIPR.
- Norma Complementar no 21/IN01/DSIC/GSIPR.
- Resolução CNJ N. 396/2021: Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Portaria CNJ N. 162/2021: Aprova os manuais da ENSEC-PJ;
- Política de Segurança da Informação do TRT14.

DESTINAÇÃO DO PROCESSO

ETIR e servidores da Secretaria de Tecnologia da Informação e Comunicação.

OUTRAS INFORMAÇÕES DESTE PROCESSO

Histórico de Revisões

Data	Versão	Descrição	Responsável
26/04/2021	1.0	Versão inicial do documento	Robson Alves Tiago
20/05/2022	1.1	Revisão do processo	Joenir José Della Flora
11/11/2022	1.2	Revisão do processo com base na auditoria Proad n. 4019/2022.	Wainner Brum Caetano
18/06/2024	1.3	Revisão do processo	Wainner Brum Caetano