PORTARIA Nº 7.791 DE 12 DE NOVEMBRO DE 2015.

Altera a Portaria nº 4.772/2008, a qual instituiu a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO os princípios constitucionais e administrativos da eficiência, eficácia e economicidade constantes do art. 37 da Constituição Federal;

CONSIDERANDO a expressiva parcela orçamentária da instituição investida em tecnologia da informação;

CONSIDERANDO a inexistência, no âmbito deste Tribunal, de formalização quanto ao processo de gerenciamento de incidentes de segurança, na área de tecnologia da informação;

CONSIDERANDO as recomendações contidas no Acórdão nº 381/2011 – Plenário do Tribunal de Contas da União, no sentido da normatização da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, bem como as informações prestadas por este Tribunal ao questionário TCU-PerfilGov 2014, quanto à implantação e formalização dos processos corporativos de segurança da informação;

CONSIDERANDO o contido no expediente administrativo nº 0000829-57.2014.5.04.0000,

RESOLVE:

Art. 1º Incluir o Anexo 8 (NSI008 – Gestão de Incidentes de Segurança da Informação) na Portaria nº 4.772/2008, com a redação constante do Anexo Único desta Portaria.

Art. 2º Republique-se a Portaria nº 4.772/2008, com as alterações promovidas pela presente.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

CLEUSA REGINA HALFEN
Presidente do TRT da 4ª Região/RS

ANEXO ÚNICO

ANEXO 8
NSI008 – Gestão de Incidentes de Segurança da Informação

1. Objetivos

Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito deste Tribunal.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

3. Referências normativas

3.1. Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.4. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um

sistema de gestão da segurança da informação dentro da organização.

3.5. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e definições

4.1. **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3. **Usuários:** magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

4.4. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.5. **Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. **Incidente de segurança da informação:** é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

4.7. **Medida de contenção:** controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o reestabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total.

4.8. **Medida de solução:** controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação.

4.9. **Tratamento de Incidentes de Segurança em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.10. **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e

redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5. Escopo

A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC, que suportam os principais processos de negócio do TRT da 4ª Região.

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes em segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

6.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste Tribunal, e dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

7. O processo de Gestão de Incidentes de Segurança da Informação

7.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

7.2.1. Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação.

7.2.2. Investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação ações de contenção, quando necessárias.

7.2.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

7.2.4. Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro,

com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.3.1. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através do formulário de solicitação de atendimento da Central de Serviços ou diretamente ao Escritório de Segurança da Informação, pelo telefone ou pelo e-mail setic.esi@trt4.jus.br, que os reportarão à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

7.3.1.1. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

7.3.1.2. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

7.3.2. As equipes da Secretaria de Tecnologia da Informação responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, para o devido registro e encaminhamento.

7.3.3. O Tribunal poderá receber notificações externas (CTIR.BR, CSIRT ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, etc, que deverão ser remetidas ao Escritório de Segurança da Informação, para o devido encaminhamento.

7.4. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.4.1. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais deve, em conjunto com as outras áreas da Setic, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenções, comunicando as áreas afetadas e coletando os dados necessários.

7.4.2. A coleta de evidências dos incidentes de segurança da informação deve ser realizada por pessoal competente e autorizado designado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ou por ela própria.

7.4.3. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.5. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRT deverão ser comunicados, para avaliação das providências cabíveis.

7.6. O encerramento do incidente de segurança da informação será realizado pelo Escritório de Segurança da Informação, com comunicação a todas as áreas interessadas, bem como ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR), na forma e nos casos definidos pelo referido órgão.

7.7. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

7.8. O desenho do processo de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo encontram-se ao final deste Anexo e dele fazem parte integrante.

8. Atualização da Norma

As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada a periodicidade prevista para a revisão da Política de Segurança da Informação.

9. Apêndices

9.1. Detalhamento dos Papéis e Responsabilidades dos envolvidos no Processo de Gestão de Incidentes de Segurança da Informação:

Papéis	
Escritório de Segurança da Informação (ESI)	Seção responsável pela área de segurança de TIC e que coordena a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI).
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	Equipe responsável pelas atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.
Comitê de Segurança da Informação	Comitê multidisciplinar responsável pela coordenação das ações e deliberações relacionadas à área de segurança da TIC.
Outras áreas da SETIC	Compreendem a Diretoria da SETIC, suas Coordenadorias e Seções. Atuam em conjunto na análise e resolução dos incidentes em redes quando acionados pela ETRI.
Presidência	Órgão diretivo do TRT a quem compete deliberar sobre as ações de contenção nos casos de incidentes graves.

Responsabilidades	
Escritório de Segurança da Informação (ESI)	Coordenar o cumprimento e evolução da maturidade do processo de Gestão de Incidentes de Segurança em Redes do Tribunal.
	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 comunicação com o CTIR.BR.
	Coordenar as atividades da ETRI do Tribunal.
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	Monitorar o ambiente e recursos de TIC do TRT a fim de perceber quaisquer alteração negativa.
	Realizar a investigação do incidente de segurança da informação, de forma a propor medidas de contenção dos danos causados pelo incidente.
	Reestabelecer a operação normal do ambiente e/ou recurso de TIC após a ocorrência de um incidente 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 de segurança da informação.
Comitê de Segurança da Informação	Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação.
Outras áreas da SETIC	Auxiliar a ETRI na proposição e execução de medidas para contenção e solução de incidentes de segurança da informação.

9.2. Detalhamento das Atividades previstas no Processo de Gestão de Incidentes de Segurança da Informação:

1. Registrar Incidente de Segurança		
Descrição	Comunicada a ocorrência ou suspeita de incidente, registrar de forma detalhada em formulário próprio no Google Drive – RISI, categorizando o incidente de segurança dentre os tipos constantes do formulário. Verificar a necessidade de autorização prévia do Comitê de Segurança de Informação para prosseguimento.	
	Atividade predecessora: não há	Atividades sucessoras: 2. Encaminhar pedido de autorização 3. Investigar o incidente
Considerações Importantes	Para o registro do incidente pode ser necessário o contato com o usuário ou equipe que o informou para esclarecimentos que permitam o registro e trâmite do incidente. Além disso, de acordo com o tipo de incidente pode ser necessária a autorização prévia do Comitê de Segurança da Informação para a realização dos procedimentos necessários à investigação.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	Comunicação de suspeita ou ocorrência de incidente de Segurança da Informação	
Saídas	Formulário RISI preenchido com informações iniciais	
Atividades	1.1 Receber a comunicação sobre o incidente	Receber e-mail, via encaminhamento do formulário de solicitação de atendimento da Central de Serviços, via formulário de registro de demanda da área técnica ou pelo envio de alertas emitidos pelos sistemas de monitoramento ou por qualquer outro meio a notificação de que ocorreu incidente de segurança ou que há suspeita de sua ocorrência.

	1.2 Solicitar esclarecimentos ao informante, quando necessário	Entrar em contato com o informante para obter informações necessárias ao registro e posterior encaminhamento das providências.
	1.3 Registrar o incidente	Preencher o Formulário RISI no Google Drive, descrevendo e categorizando o incidente.
	1.4 Verificar necessidade de autorização prévia do Comitê de Segurança da Informação	Após categorizar o incidente, verificar a necessidade de autorização do Comitê de Segurança da Informação para o prosseguimento. Em geral, são submetidas à prévia autorização do Comitê a emissão de relatórios de acesso de determinado servidor em sistemas e serviços disponibilizados, investigações de acessos não autorizados ou que exijam a verificação de dados dos usuários.
	1.5 Encaminhar para o Escritório de Segurança da Informação	Se necessária autorização do Comitê, encaminhar ao Escritório de Segurança da Informação para solicitar a autorização.
	1.6 Encaminhar incidente para investigação	Após autorização do Comitê ou quando desnecessária autorização, encaminhar o incidente para investigação pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI). Este encaminhamento poderá ser direcionado a apenas um dos integrantes da equipe, quando se trate de ação específica para cuja realização o integrante esteja habilitado.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

2. Encaminhar pedido de autorização		
Descrição	Ao Escritório de Segurança da Informação incumbe solicitar autorização ao Comitê 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.	
	Atividade predecessora: 1. Registrar o incidente de segurança	Atividades sucessoras: 3. Investigar o incidente 9. Cumprir providências/encerrar o incidente
Considerações Importantes	O funcionamento do Comitê de Segurança da Informação está regrado no Anexo 5 da Política de Segurança da Informação. Aspectos importantes: O quórum mínimo para deliberação no Comitê é de três magistrados e dois servidores. Nas ausências do Presidente do Comitê quem o substitui é o Juiz Auxiliar da Presidência. As deliberações podem ser feitas por meio eletrônico (e-mail).	
Papéis	Escritório de Segurança da Informação	
Entradas	Formulário RISI – com registro de incidente que necessita de relatórios de acesso de determinado servidor	
Saídas	Pedido de autorização ao Comitê de Segurança da Informação (por e-mail)	
Atividades	2.1. Coletar as informações necessárias ao encaminhamento do pedido de autorização para prosseguimento da investigação	Ao encaminhar o pedido de autorização para prosseguimento da investigação, o Escritório de Segurança da Informação deve fornecer ao Comitê de Segurança da Informação o máximo de informações possíveis que propiciem a deliberação de forma rápida.
	2.2. Encaminhar pedido de autorização ao Comitê	O pedido de autorização pode ser encaminhado via e-mail ou submetido para deliberação em reunião do Comitê de Segurança da Informação.

	2.3. Prestar os esclarecimentos, quando necessário	O Comitê de Segurança da Informação poderá solicitar esclarecimentos antes da autorização. Neste caso, o Escritório de Segurança da Informação é o responsável por coletar as informações e encaminhá-las ao Comitê.
	2.4. Encaminhar para investigação	Se autorizado, o Escritório de Segurança da Informação deve dar prosseguimento à investigação junto à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI).
	2.5 Encaminhar para finalização	Nos casos em que não houver autorização pelo Comitê de Segurança da Informação para a realização da investigação solicitada, encaminhar para finalização ou encerramento do incidente.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

3. Investigar o incidente		
Descrição	A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), com base nas informações registradas no RISI, 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.	
	Atividades predecessoras: 1. Registrar incidente de segurança 2. Encaminhar incidente de segurança	Atividades sucessoras: 4. Propor ações de contenção 5. Comunicar as áreas afetadas 6. Realizar investigação de acessos Estas atividades poderão ocorrer de forma concomitante ou não.
Considerações Importantes	Para esta atividade a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) poderá solicitar informações às áreas técnicas responsáveis, a fim de elucidar a extensão e o impacto do problema, quais ativos e sistemas estão sendo afetados e começar a definir uma ação para conter o incidente. A identificação do tipo e impacto do incidente é muito importante nesta etapa, pois ela definirá o encaminhamento a ser dado quanto à necessidade de ações de contenção, de comunicação a outras áreas sobre a ocorrência do incidente e de realização de investigação de acessos.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	Autorização do Comitê de Segurança da Informação ou Formulário RISI preenchido com as informações iniciais	
Saídas	Formulário RISI preenchido com as informações do incidente investigado	
Atividades	3.1 Verificar o tipo de incidente	Verificar se é uma investigação de acesso indevido, descumprimento da Política de Segurança da Informação, indisponibilidade de um serviço ou sistema por falha de segurança, invasão, propagação de vírus, vazamento de dados etc.
	3.2 Analisar a extensão e o impacto causado pelo incidente	Analisar quais serviços, sistemas e ativos foram afetados e qual foi o dano causado pelo impacto. Se necessário, envolver outras equipes.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

4. Propor ações de contenção		
Descrição	Com base nas informações levantadas na investigação do incidente, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá propor ações para conter o incidente, que podem ser soluções de contorno ou de resolução do problema.	
	Atividades predecessoras: 3. Investigar o incidente 7. Aplicar medidas aprovadas	Atividade sucessora: 7. Aplicar medidas aprovadas
Considerações Importantes	Dependendo do tipo de incidente e de sua extensão, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) poderá envolver outras áreas da Setic para definir as ações de contenção. Dependendo da ação que for definida e da gravidade do incidente, poderá ser necessária a aprovação da chefia de uma ou mais áreas envolvidas ou mesmo da Presidência do Tribunal. Se as medidas não forem autorizadas, novas medidas deverão ser propostas. Assim também se o incidente não for contido, novas medidas deverão ser propostas.	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com as informações sobre o incidente/ ou não aprovação das medidas anteriores/ ou informação de que as medidas não foram suficientes a conter o incidente	
Saídas	RISI preenchido com as ações de contenção propostas	
Atividades	4.1 Propor ações de contenção	A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá propor ações que contenham o incidente, de forma a evitar que os danos e impactos aumentem com o passar do tempo. Além disso, a ação de contenção deve reestabelecer o sistema ou serviço, ainda que parcialmente, via solução de contorno ou resolução da causa do incidente.
	4.2 Encaminhar solução para aprovação das chefias	Dependendo do teor da ação proposta, será necessária a aprovação da chefia das áreas afetadas e/ou envolvidas no incidente e na sua resolução.
	4.3. Proposição de novas medidas, caso o incidente não seja contido	Se o incidente não for contido pelas medidas inicialmente propostas, novas medidas deverão ser estudadas e aplicadas.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

5. Comunicar as áreas afetadas		
Descrição	Se o incidente de segurança afetar um ou mais grupos de serviço/sistemas ou usuários (por exemplo, investigação de acesso por descumprimento da Política de Segurança da Informação), a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), de posse da extensão e do impacto do incidente, deverá comunicar as áreas da Setic sobre a ocorrência e, em conjunto com o Escritório de Segurança da Informação, deliberar se é necessário informar outras áreas do TRT sobre o incidente.	
	Atividade predecessora: 3. Investigar o incidente	Atividade sucessora: 4. Propor ações de contenção
Considerações Importantes	É de suma importância informar outras áreas da Setic para que estas possam agir para ajudar na proposição de medidas para conter e/ou resolver o incidente. Além disso, a área de Atendimento aos Usuários deve ser informada principalmente quando o incidente afetar sistemas e serviços utilizados diretamente pelos usuários, de forma a repassar orientações e informações sobre o incidente e seu tratamento, prazo de retorno do serviço, etc. Se necessário, uma comunicação ostensiva pode ser divulgada, informando que a Setic está ciente do problema e está trabalhando para resolvê-lo, estimando o tempo para tratá-lo.	

Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com as informações sobre o incidente investigado	
Saídas	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 comunicações.	
Atividades	5.1. Informar a extensão do impacto e quais sistemas/ serviços foram afetados	De posse dessas informações, será possível avaliar a quem e como a comunicação será realizada, bem como o teor da mensagem.
	5.2. Definir como e a quem a comunicação será realizada	Definir, em conjunto com o Escritório de Segurança da Informação, como a mensagem será divulgada, a quem será divulgada e o que ela conterá.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

6. Coletar dados (relatório de acessos)		
Descrição	Se o incidente disser respeito à investigação sobre acessos de determinado(s) servidor(es) em sistemas e serviços disponibilizados, investigação de acessos não autorizados ou que exijam a verificação de dados dos usuários, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) realizará a auditoria necessária e compilará os dados em relatório a ser encaminhado ao Comitê de Segurança da Informação.	
	Atividade predecessora: 3. Investigar o incidente	Atividade sucessora: 8. Analisar incidente
Considerações Importantes	Nestes casos a documentação gerada deverá ser armazenada em local de acesso restrito (os relatórios não deverão ser inseridos no sistema utilizado para o registro dos incidentes e demandas em geral).	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI + Autorização do Comitê de Segurança da Informação	
Saídas	Relatório de acessos	
Atividades	6.1. Identificação dos dados necessários à elucidação do incidente	De acordo com as informações recebidas os dados podem ser coletados de sistemas de monitoramento diversos. Assim é importante que sejam identificados quais os dados que melhor podem elucidar a questão noticiada.
	6.2. Realizar a coleta e compilação de dados	Realizar a coleta e a compilação de dados necessários à elaboração de relatório ao Comitê de Segurança da Informação. Estes dados deverão ser armazenados em local de acesso restrito ao Escritório de Segurança da Informação ou ao Comitê.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação.	

7. Aplicar medidas aprovadas		
Descrição	Executar as ações propostas na fase anterior, visando conter o incidente, e verificar se o resultado esperado foi alcançado.	
	Atividade predecessora: 4. Propor ações de contenção (caso as medidas aplicadas não tenham sido suficientes a conter o incidente de forma adequada).	Atividade sucessora: 8. Analisar incidente

Considerações Importantes	Após aplicar as medidas, a equipe deverá avaliar se o incidente foi contido e, em caso negativo, deverá propor/realizar novas ações que contenham o incidente.	
Papéis	Outras áreas da Setic e Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI com autorização da aplicação da medida de contenção proposta	
Saídas	RISI com resultados das medidas aplicadas	
Atividades	7.1 Aplicar as medidas necessárias	Realizar as configurações e/ou modificações necessárias para conter o incidente.
	7.2 Avaliar medidas aplicadas	Verificar se medidas aplicadas obtiveram o resultado esperado e, em caso negativo, propor novas medidas de contenção.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

8. Analisar incidente		
Descrição	Esta atividade tem por objetivo 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). Se for o caso de uma investigação (suspeita de violação da Política de Segurança da Informação), a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê de Segurança da Informação.	
	Atividades predecessoras: 6. Coletar dados (relatórios de acesso) 7. Aplicar medidas aprovadas	Atividades sucessoras: 9. Analisar proposições ESI 10. Cumprir providências/encerrar o incidente
Considerações Importantes	O estudo poderá ser realizado em conjunto com outras áreas dependendo do tipo de incidente. De acordo com o teor da proposição, poderá ser necessário o encaminhamento para deliberação por parte do Comitê de Segurança da Informação ou comunicação a outras áreas (internas e externas).	
Papéis	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Entradas	RISI preenchido com todas as informações	
Saídas	Solicitação de manifestação do Comitê de Segurança da Informação // Proposição de ações à Direção da Setic.	
Atividades	8.1 Analisar causa-raiz do incidente	Analisar o cenário do incidente, identificando a causa-raiz, quais as vulnerabilidades exploradas, quais as ameaças envolvidas, etc;
	8.2 Propor melhorias no cenário investigado	De posse da análise realizada, propor ações de melhoria para o cenário analisado, de forma a evitar (ou diminuir o risco de) que o incidente volte a ocorrer.
	8.3 Redigir relatório	No caso de ser uma investigação de acessos, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI) deverá analisar logs e utilizar as ferramentas de auditoria disponíveis para elucidar a suspeita informada no RISI e encaminhar o relatório à apreciação do Comitê de Segurança da Informação.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

9. Analisar proposições ETRI		
Descrição	Avaliar as soluções propostas ou analisar o relatório de auditoria enviado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), deliberando a respeito ou simplesmente tomando ciência acerca do incidente, quando for o caso.	
	Atividade predecessora: 8. Analisar incidente	Atividade sucessora: 10. Cumprir providências/encerrar o incidente
Considerações Importantes	Nos casos de auditoria de logs de determinado usuário, o Comitê de Segurança da Informação analisará o teor do relatório e deliberará sobre o encaminhamento assunto do qual o mesmo trata. Outras questões também podem ser submetidas ao Comitê, considerando o impacto e abrangência do incidente.	
Papéis	Comitê de Segurança da Informação	
Entradas	Proposição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)	
Saídas	Deliberação do Comitê de Segurança da Informação	
Atividades	9.1. Tomar ciência do incidente e medidas aplicadas	Tomar ciência do incidente e das medidas aplicadas.
	9.2 Avaliar soluções propostas	Ao Comitê de Segurança da Informação cabe deliberar sobre a proposição de novas ações pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), sempre que necessária sua intervenção.
	9.3. Analisar relatório de investigação/auditoria	Analisar o relatório e deliberar sobre o encaminhamento a ser dado.
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

10. Cumprir providências/encerrar o incidente		
Descrição	O Escritório de Segurança da Informação deverá encaminhar para a equipe responsável as ações de melhorias levantadas e aprovadas, de forma a contribuir para que o problema seja resolvido. Além disso, caso haja alguma ação a ser tomada, informada pelo Comitê de Segurança da Informação na fase anterior, o Escritório de Segurança da Informação deverá executar durante esta fase. Depois, o incidente de segurança da informação será considerado como encerrado.	
	Atividades predecessoras: 8. Analisar incidente 9. Analisar proposições ESI	Atividade sucessora: 11. Analisar e consolidar informações (alimentar indicadores)
Papéis	Escritório de Segurança da Informação	
Entradas	Deliberação do comitê // RISI com providências	
Saídas	RISI preenchido e encerrado // Notificação ao CTIR.BR	
Atividades	10.1 Cumprir providências	O Escritório de Segurança da Informação deverá dar prosseguimento nas deliberações e ações definidas pelo Comitê de Segurança da Informação ou pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI)
	10.2 Encerrar o incidente	Nesta fase, o incidente deve ser encerrado, uma vez que ele foi analisado e tratado corretamente.

	10.3 Notificar o incidente ao CTIR.BR	O incidente deverá ser informado ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR.BR (ver documento NOTIFICAÇÃO CTIR-Procedimentos)
Modelo de documento	RISI – Relatório de Incidente de Segurança da Informação	

11. Avaliar histórico de incidentes e consolidar informações (alimentar indicadores)		
Descrição	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 riscos, bem como sistema ou serviço afetado por um ou mais incidentes.	
	Atividade predecessora: 10. Cumprir providências/encerrar o incidente	Atividade sucessora: 12. Verificar oportunidades de melhoria e lições aprendidas
Considerações Importantes	É importante que os RISIs sejam preenchidos de forma completa e precisa, pois serão utilizados para alimentar os indicadores do processo de gestão de riscos.	
Papéis	Escritório de Segurança da Informação	
Entradas	RISI encerrado	
Saídas	Registro de indicadores	
Atividades	11.1 Avaliar histórico de incidentes	Verificar os RISIs anteriores e outras bases (TraceGP, por exemplo) a fim de fazer alguma correlação de incidentes e verificar possíveis *gaps* em algum processo, sistema ou infraestrutura.
	11.2 Alimentar indicadores estabelecidos	Atualizar as informações dos indicadores definidos para o processo.

12. Verificar oportunidades de melhoria e lições aprendidas		
Descrição	Com base na análise e consolidação de informações dos indicadores, deve-se buscar *gaps* no processo de gestão de incidentes e serviços/sistemas afetados pelos incidentes, para então sugerir melhoria nos mesmos.	
	Atividade predecessora: 11. Avaliar histórico de incidentes e consolidar informações	Atividade sucessora: Não há
Papéis	Escritório de Segurança da Informação	
Entradas	Registro de indicadores	
Saídas	Relatório de melhorias	
Atividades	12.1 Analisar indicadores	Com base nos indicadores e avaliação junto às outras áreas, o Escritório de Segurança da Informação deve avaliar se o processo está eficaz.
	12.2 Propor melhorias no processo	De acordo com a avaliação do processo e análise dos indicadores, o Escritório de Segurança da Informação deverá propor melhorias para tornar o processo mais eficaz e objetivo.

9.3. Modelos de Documentos a serem utilizados nas atividades previstas no

PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

Processo de Gestão de Incidentes de Segurança da Informação:

9.3.1. RISI – Relatório de Incidentes de Segurança da Informação

RISI – Relatório de Incidente de Segurança da Informação	
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – Tribunal Regional do Trabalho da 4ª Região	
1 – Informações do RISI	
Descrição do Incidente:	Data e Hora de abertura:
	Data e Hora de fechamento:
Severidade do Incidente: ☐ Alta ☐ Média ☐ Baixa	
2 – Identificador do Incidente	
Origem da Identificação: ☐ Interna ☐ Externa	
Nome Completo:	
Área/Seção:	
Telefone:	
E-mail:	
Empresa: N/A	
3 – Detalhamento do Incidente	
Tipo de Incidente	**Descrição detalhada do incidente de Segurança**
Não conformidade com a PSI ☐ Utilização da Internet ☐ Utilização do e-mail ☐ Utilização de Recurso Computacional	
Indisponibilidade de Serviço ou Sistema ☐ Rede ☐ E-mail ☐ Internet ☐ PJe-JT ☐ ADMEletrônico ☐ inFOR ☐ Link de dados ☐ Outros _____	
☐ **Ataque de força bruta a um sistema/página web**	
☐ **Alteração de sistema não planejada**	
☐ **Infecção por *malware***	
***Defacement* (alteração não autorizada de portal)**	

☐ Internet ☐ Intranet ☐ Extranet	
DoS (Negação de Serviço) ☐ Portal de Internet ☐ Link de dados ☐ Sistemas	
☐ **Outros** Informar:	

Tipo de Impacto do Incidente	**Grau de Impacto**
☐ Confidencialidade	☐ Baixo ☐ Médio ☐ Alto
☐ Integridade	☐ Baixo ☐ Médio ☐ Alto
☐ Disponibilidade	☐ Baixo ☐ Médio ☐ Alto

4 – Investigação do Incidente

Equipe responsável pela investigação:	**Descrição detalhada da Investigação (causa raiz, o que ocasionou o incidente, etc.)**
Data de Entrega do Plano de Investigação:	

5 – Ação de Contenção

Equipe responsável pela execução da ação:	**Descrição da Ação de Contenção:**
Outras áreas envolvidas:	
Data e hora de proposição da ação:	
Data e hora de execução da ação proposta:	
Responsável(is) pela aprovação:	

6 – Comunicação a partes interessadas

Informar a quem o incidente foi comunicado	**Data e hora da comunicação**	**Pessoa comunicada**	**Meio de comunicação**
☐ SETIC			
☐ ESI			

☐ CPP			
☐ CDS			
☐ CIT			
☐ CAU			
☐ Partes interessadas ou afetadas. Informar:			
☐ Outros. Informar:			

7 – Análise e Encerramento do RISI

Outras ações necessárias? ☐ Sim ☐ Não	**Descrição Detalhada da(s) ação(ões) proposta(s)**
Responsável pela ação:	
Data de Proposição da Ação:	

9.3.2. Registro de Indicadores:

Registro de Indicadores		
Indicadores	**Ano 1**	**Ano 2**
Quantidade de incidentes registrados		
Quantidade de incidentes resolvidos		
Quantidade de incidentes em andamento		
Quantidade de incidentes registrados – por nível de severidade (alta, média e baixa)		
Quantidade de incidentes registrados – por categoria (não conformidade com a PSI, indisponibilidade de serviço/sistema, ataque de força bruta, infecção por *malware*, alteração não-autorizada de portal, negação de serviço)		

9.3.3. Notificação CTIR.BR – Procedimentos

NOTIFICAÇÃO CTIR.BR – PROCEDIMENTOS

1. A comunicação entre órgãos e instituições da APF e o CTIR Gov deve ocorrer por meio das ETIR, de forma centralizada, preferencialmente por meio de e-mail institucional relacionado a incidentes de segurança. No caso do TRT4 será utilizado o e-mail do Escritório de Segurança da Informação (posteriormente, poderá ser implementada nova conta específica abuse@orgao.gov.br, como sugerido nos padrões do CTIR).

2. O ponto único de contato para as notificações de incidentes de segurança ao CTIR Gov é o endereço eletrônico: ctir@ctir.gov.br.
    1. Para comunicação através de um canal seguro, deverá ser utilizada a seguinte chave PGP:
       PGP Key ID: 0xAFBEDFCF
       Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF
    2. O CTIR Gov atende ainda pelo telefone INOC-DBA: 10954*810.

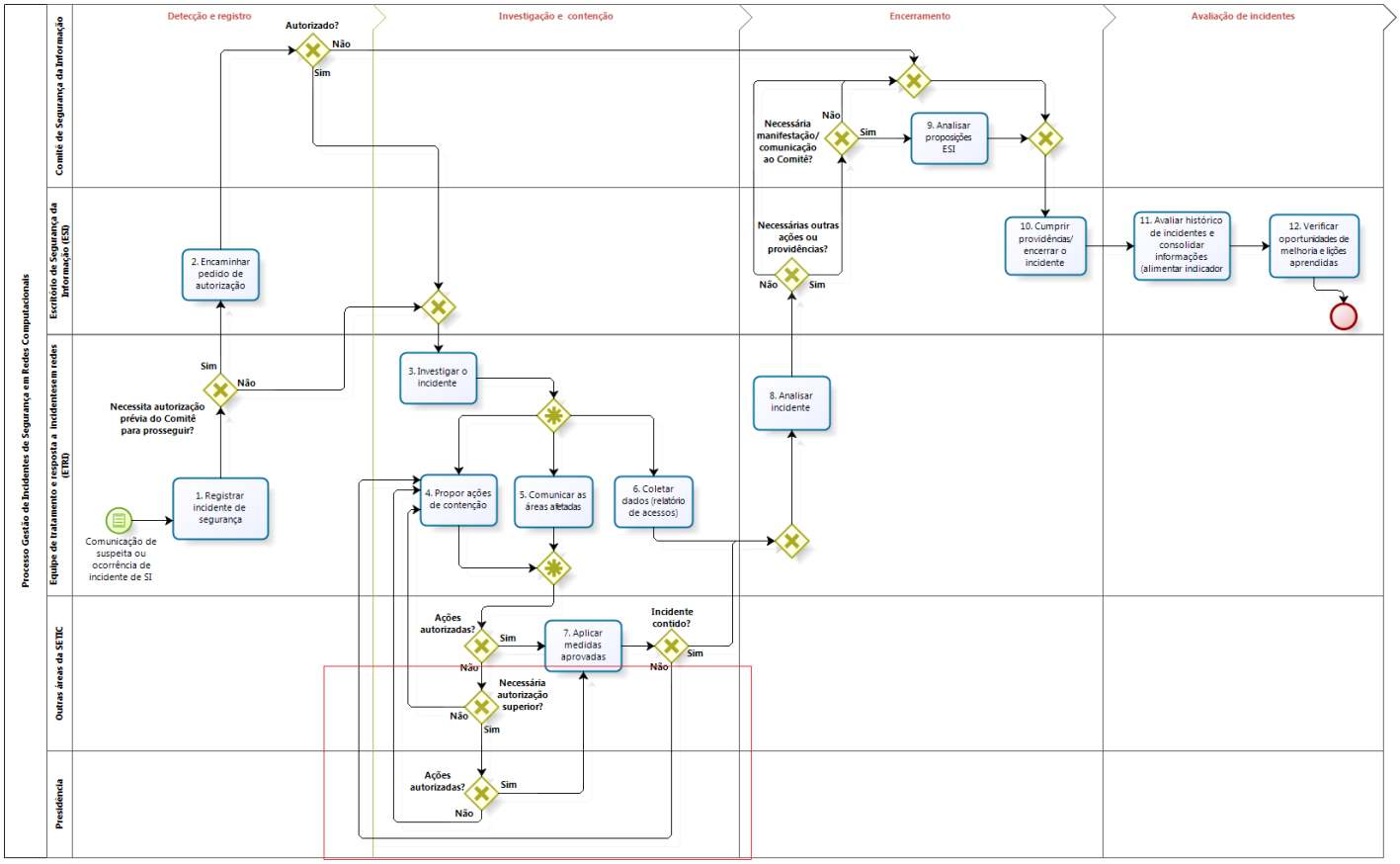
3. As questões gerenciais ou relacionadas à Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR) serão tratadas por meio do correio eletrônico: cgtir@planalto.gov.br.

4. A notificação deverá conter os seguintes dados:
    1. Assunto: fazer constar o "*nome do órgão*" e o "*tipo do incidente*".
    2. Destinatário: ctir@ctir.gov.br.
    3. CC: eventualmente, podem ser copiados outros envolvidos no incidente.
    4. Corpo da Notificação: descrever sucintamente o incidente ocorrido, atentando para a correção das informações, tais como: organizações, pessoas ou serviços de rede envolvidos; time zone; registros de log; cronologia dos acontecimentos; ações adotadas; outros detalhes técnicos e incidentes correlacionados.
    5. Anexos: Deverão ser anexadas as informações que facilitem a análise e a resposta ao incidente, tais como: logs de servidores e/ou serviços, cabeçalho de mensagens, código malicioso, etc.

3. No caso de recebimento de uma notificação ou resposta do CTIR, nas Comunicações que se seguirem deve sempre ser referenciado no campo "*Assunto*" o número de identificação fornecido no formato [CTIR Gov BR #XXXXX].

4. Principais tipos de incidentes de segurança possíveis de serem notificados:
    1. abuso de sítios (desfiguração, injeção de links/código – *spamdexing*, erros de código, *cross site scripting*, abuso de fórum ou livros de visita, etc.);
    2. inclusão remota de arquivos (*remote file inclusion* – RFI) em servidores web;
    3. uso abusivo de servidores de e-mail;
    4. hospedagem ou redirecionamento de artefatos ou código malicioso;
    5. ataques de negação de serviço;
    6. uso ou acesso não autorizado a sistemas ou dados;
    7. varredura de portas;
    8. comprometimento de computadores ou redes;
    9. desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia;
    10. ataques de engenharia social – *phishing*; (no caso de *phishing* recebido por e-mail, solicita-se que, além do texto da mensagem, sejam enviados os cabeçalhos completos para que se proceda, dentre outras coisas, à notificação do servidor de e-mail comprometido);
    11. cópia e distribuição não autorizada de material protegido por direitos autorais;
    12. uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

9.4. Desenho do Processo de Gestão de Incidentes de Segurança da Informação:



PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS
TRT DA 4ª REGIÃO