Poder Judiciário
Justiça do Trabalho
Tribunal Regional do Trabalho da 16ª Região

PORTARIA GP nº 671/2017 São Luís, julho de 2017.

Institui o Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA SEXTA REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO Auditoria do Conselho Superior de Justiça do Trabalho realizada neste Tribunal, conforme processo CSJT-A-26207-89.2015.5.90.0000, PA TRT16 nº 3741/2015, que verificou a inexistência de processos críticos que compõe um Sistema de Gestão de Segurança da Informação, em seu item 2.14.,

CONSIDERANDO a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n. 211, de 15 de dezembro de 2015;

CONSIDERANDO a publicação pelo Conselho Nacional de Justiça de diretrizes gerais para a implantação da Gestão de Segurança da Informação no Poder Judiciário;

CONSIDERANDO a importância do Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação para este Tribunal e seu alinhamento com o PETIC (Planejamento Estratégico de Tecnologia da Informação e Comunicação 2017-2020);

CONSIDERANDO as diretrizes, requisitos e práticas apontadas pelas normas NBR ISO/IEC 27000, 27001, 27002 e 27003.

R E S O L V E

Art. 1º Instituir o Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região, conforme Anexo I desta Portaria.

Art. 2º Esta Portaria produzirá seus efeitos a contar da data de sua publicação.

São Luís, julho de 2017.

(assinado eletronicamente)
Des. JAMES MAGNO ARAUJO FARIAS
Presidente do TRT da 16ª Região

/CTIC

TRIBUNAL REGIONAL DO
TRABALHO DA 16ª REGIÃO

ANEXO I

Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação

Julho/2017

Sumário

1. Objetivo

Este documento tem por objetivo estabelecer o Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região (TRT16).

A Gestão de Incidentes de Segurança da Informação é um dos requisitos elencados na ISO/IEC/NBR 27001, norma de padrão internacional que trata de requisitos relacionados à segurança da informação.

No âmbito do TRT16, este processo visa fornecer respostas efetivas às ameaças que possam comprometer a efetividade na execução da sua missão institucional que é “Realizar justiça no âmbito trabalhista”.

2. Aplicabilidade

O Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação tem aplicabilidade:

- em toda informação produzida, armazenada ou transmitida pelo e entre o TRT16 e outras entidades;
- em todos os sistemas, serviços, equipamentos de TI e de telecomunicações que sejam utilizados ou providos por este Tribunal, inclusive aqueles que pertençam a terceiros;
- para todas as pessoas que lidem com informações deste órgão, mesmo aquelas de outras entidades, aquelas fora das dependências do Tribunal, aquelas em trânsito e aquelas em regime de teletrabalho;

3. Referências Normativas

A elaboração do processo descrito por este documento utilizou como referência as seguintes normas:

- ABNT NBR ISO/IEC 27000:2014;
- ABNT NBR ISO/IEC 27001:2013;
- ABNT NBR ISO/IEC 27002:2013;
- ABNT NBR ISO/IEC 27003/2011:

4. Termos e Definições

Termos e definições não especificados nesta seção terão o seu significado esclarecido pela norma ABNT NBR ISO/IEC 27000.

Ameaça	É a causa potencial de um incidente de segurança da informação. Exemplo: pessoas interessadas em obter acesso a processos em segredo de justiça, pessoas interessadas em obter antecipadamente votos ou sentenças judiciais, pessoas interessadas em coletar dados pessoais de servidores e magistrados, pessoas interessadas em manchar a reputação da Tribunal, dentre outros.
Ativo	Tudo que represente algum tipo de valor para o negócio da organização e que, por isso, precise ser protegido. Por exemplo: um documento em papel, um documento digital, um sistema, um equipamento, uma gravação, etc.
Conformidade	Cumprir um requisito que pode ser técnico, processual ou até mesmo legal. Exemplo: conformidade com o processo de monitoramento e tratamento de incidentes, conformidade com a Lei de Acesso à Informação, conformidade com as boas práticas de *baseline* da Microsoft para o Active Directory.
Contato institucional	Contato estabelecido entre o TRT16 e órgãos externos, como provedores de acesso, empresas, órgãos governamentais, polícia, dentre outros.
Evento	Ocorrência ou alteração de um determinado conjunto de circunstâncias de um ambiente. Eventos podem ser positivos (melhorias, correções), negativos (incidentes, problemas) ou mesmo comportamentos normais como o simples fato de um sistema informar ao administrador que está funcionando normalmente.
Evidências	São artefatos que podem ser usados para analisar o incidente, identificar a origem de ataques e atribuir responsabilidades. São exemplos de evidências: logs, documentos físicos, documentos digitais, imagens, gravações, dentre outros.
Exploração da vulnerabilidade	É sinônimo de ataque. A exploração da vulnerabilidade ocorre quando a ameaça ataca um ativo e tenta destruir, expor, alterar ou obter acesso não autorizado a informações através de vulnerabilidades existentes.
Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação	É um grupo formado para atuar na solução de incidentes de segurança da informação.
Incidente	Qualquer acontecimento que não seja parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção ou redução na qualidade daquele

	serviço. Por exemplo: mau funcionamento de um computador, lentidão no acesso à Internet, problemas no uso do PJe.
Incidente de Segurança da Informação	É um tipo específico de incidente relacionado à segurança da informação. Por exemplo: roubo de senhas de e-mail, infecção de um computador por vírus, violação da Política de Segurança da Informação e Comunicações (POSIC), ausentar-se do computador sem bloqueá-lo.
Índice	É aquilo que se deseja medir. Por exemplo: quantidade de incidentes por mês, percentual de ataques com origem identificada, etc.
Meta	É o valor de um índice que se deseja alcançar. Por exemplo: criar pelo menos 3 conhecimentos por mês, identificar pelo menos 30% da origem dos ataques, realizar pelo menos, implementar 2 controles da norma NBR/ISO/IEC 27002 por semestre.
Parte interessada	Consiste na pessoa ou na organização que pode afetar, ser afetada ou que vislumbra ser afetada por uma decisão ou atividade ligadas ao incidente de segurança da informação. Exemplo: provedor de acesso, diretoria geral, coordenador da CTIC, Polícia Federal, CERT.br, dentre outros.
Processo	Se refere aos processos/fluxos relacionados à segurança da informação.
Requisito	Consiste numa exigência que deve ser atendida para que algo ou alguém esteja em conformidade com algum critério técnico, processual ou legal.
Solucionar incidente	Consiste em realizar uma ação para reestabelecer o funcionamento normal do ambiente. Sempre que possível, a solução do incidente contemplará a correção da vulnerabilidade e as ações para evitar a proliferação do ataque para outros pontos da organização.
Vulnerabilidade	É um ponto fraco no elo da segurança da informação que, se explorada, poderá causar danos à organização. Por exemplo: não haver criptografia ou hash de senhas no banco de dados, não usar HTTPs em páginas que transitam dados sigilosos, deixar senhas anotadas em papéis sobre a mesa, dentre outros.

5. Papéis e Responsabilidades

Papel	Responsabilidade
Tribunal Pleno	• Aprovar alterações na Política de Segurança da Informação e Comunicação (POSIC);

Presidente do Tribunal	• Estabelecer, quando necessário, contato institucional com órgãos externos; • Resolver casos omissos ao Comitê Gestor de Segurança da Informação e Comunicação;
Comitê Gestor de Segurança da Informação e Comunicação (CGSIC)	• Estabelecer diretrizes e estratégias para as ações de segurança da informação; • Analisar relatórios; • Constituir grupos de trabalho; • Apreciar normas e procedimentos; • Decidir sobre índices e metas; • Apreciar sugestões de novos processos ou de melhorias em processos já existentes;
Seção de Segurança e Inteligência Institucional	• Prover a segurança física; • Prover o vídeo monitoramento; • Apoiar as iniciativas da Seção de Segurança da Informação e do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação;
Usuários	• Notificar a Seção de Segurança da Informação sobre violação ou suspeitas de violação à PSI; • Obedecer à Política de Segurança da Informação e Comunicação; • Fornecer informações necessárias ao tratamento de incidentes em que esteja envolvido;
COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES (CTIC)	
Coordenador da CTIC	• Decidir, em última instância, sobre a alocação de recursos humanos e materiais da CTIC necessários ao tratamento de incidentes de segurança da informação; • Intermediar o diálogo com a alta administração;
Chefe da Seção de Segurança da Informação (SSI)	• Emitir relatórios gerenciais; • Realizar o contato com as demais unidades da CTIC; • Coordenar as atividades do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação e da Seção de Segurança da Informação; • Manter-se informado sobre os incidentes durante todo o seu ciclo de vida; • Manter o Coordenador da CTIC informado sobre os incidentes;

Analista da Seção de Segurança da Informação	• Iniciar, conduzir e encerrar a execução do processo de tratamento; • Apoiar o Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação; • Avaliar e validar a conformidade da atuação do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação; • Estabelecer contato com unidades de TI ou de Segurança da Informação externas, quando houver necessidade; • Classificar os eventos e registrar as informações pertinentes ao escopo da sua função; • Manter todas as partes envolvidas informadas; • Emitir sugestões de melhorias;
Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação	• Decidir sobre os procedimentos técnicos a serem adotados na resposta a incidentes da informação; • Diligenciar para coletar e proteger evidências; • Solucionar e documentar incidentes; • Manter a SSI informada sobre o status do incidente;
Unidades da CTIC	• Fornecer apoio humano especializado para compor o Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação • Notificar a SSI sobre eventos com potencial de serem incidentes de segurança da informação; • Reassumir o evento quando a SSI não o classificar como incidente de segurança da informação; • Analisar criticamente e sugerir a forma de aplicação das recomendações da SSI;

6. Interface com outros processos

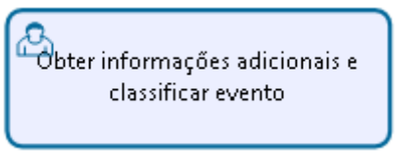
A seguir estão descritas as principais interfaces do Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informações com os demais processos de gestão de TIC do TRT16 e sua importância para o gerenciamento dos serviços de TI:

- **Gerenciamento de Incidentes:** quando um evento não for classificado em incidente de segurança da informação, o processo de gerenciamento de incidentes deve ser acionado para a resolução do evento.

7. Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação

O processo encontra-se desenhado no Anexo I deste documento.

 Receber notificação de evento suspeito	**Receber notificação de evento suspeito**
Objetivo: Receber a notificação de um evento que potencialmente represente um incidente de segurança da informação.	
Entradas: • Chamado/ticket; • Notificação recebida de uma entidade externa (CERT.br, CSJT, CNJ, provedores de acesso, etc); • Atividade proativa das unidades da CTIC;	
Descrição da atividade: Receber a notificação de um evento. Se o evento não estiver registrado na Central Atendimento, proceder com o seu registro. Se registrado, dar sequência ao fluxo do processo.	
Responsável: Seção de Segurança da Informação (SSI).	
Saída: Chamado/ticket	

	**Obter informações adicionais e classificar evento**

Objetivo:

Filtrar eventos não relacionados à segurança da informação e coletar informações para conhecer a dimensão do incidente e subsidiar as primeiras ações do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação.

Entradas:

Chamado recebido pela SSI;

Descrição da atividade:

1. Diligenciar na busca por informações adicionais;
2. Classificar o evento;

Responsável:

Analista da SSI;

Saída:

- Registro de informações no chamado/ticket;
- Chamado/ticket classificado.

	**Comunicar as partes interessadas**

Objetivo:

Garantir que as informações sejam comunicadas às pessoas ou entidades que irão se beneficiar delas ou que necessitem agir com base nelas.

Entradas:

Chamado/ticket

Descrição da atividade:

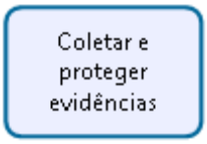
1. Identificar as partes interessadas;
2. Comunicar o conteúdo adequado para sua respectiva parte interessada, como por exemplo:
    a. dados preliminares do incidente;
    b. ações iniciais;
    c. potenciais impactos e cuidados a serem tomados;
    d. dados que possam ser relevantes na contenção ou não proliferação do incidente em questão.

Responsável:

Analista da SSI.

Saída:

- Chamado/ticket;

	**Coletar e proteger evidências**

Objetivo:

Preservar as evidências para análise técnica, estudos e, se necessário, responsabilização;

Entradas:

Chamado/ticket classificado como incidente de segurança da informação.

Descrição da atividade:

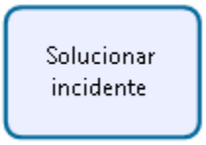
1. Diligenciar em busca de evidências que possam subsidiar a análise do incidente;
2. Se a evidência for digital, armazená-la em sistema próprio para este fim;
3. Se a evidência for física, colhê-la com o apoio das unidades competentes, inclusive a Coordenadoria de Material e Patrimônio, a Seção de Segurança e Inteligência Institucional e, se necessário, com entidades externas;
    a. Manter a evidência física sob custódia da Seção de Segurança e Inteligência Institucional, instruindo-a sobre a sensibilidade dos dados e os cuidados no armazenamento dos mesmos;

Responsável:

Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação.

Saída:

- Evidências como logs, prints screens, e-mails, gravações em áudio e vídeo, papéis, imagens, fotografias, equipamentos, mídias digitais e dispositivos de armazenamento interno e externo, etc.

	**Solucionar incidente**

Objetivo:

Conter a ameaça e que deu causa ao registro do incidente de segurança da informação.

Entradas:

- Chamado/ticket;
- Evidências;

Descrição da atividade:

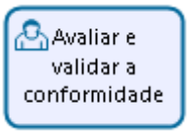
1. Consultar base de conhecimento;
2. Checar os riscos e tomar ações para reduzir aqueles de maior impacto;
3. Intervir para cessar a exploração da vulnerabilidade;
4. Emitir recomendações e esclarecimentos para os usuários, quando necessário;
5. Reestabelecer a normalidade para os sistemas e informações;
6. Registrar informações no chamado e na base de conhecimento;
7. Se possível, identificar a origem do ataque;
8. Sugerir melhorias;
9. Validar a solução adotada;
10. Reassumir o chamado caso ele não tenha sido solucionado;

Responsável:

Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação.

Saída:

- Chamado/ticket resolvido;
- Recomendações e esclarecimentos para os usuários, quando necessário;

	**Avaliar e validar a conformidade**

Objetivo:

Avaliar a execução do tratamento e resposta do incidente no que tange ao cumprimento das leis, políticas, normas, regulamentações, processos, procedimentos e boas práticas.

Entradas:

Chamado/ticket com informações do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação.

Descrição da atividade:

1. Primordialmente, checar o cumprimento do Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação;
2. Checar o cumprimento dos requisitos internos e externos que tangem o tratamento de incidentes de segurança da informação;
3. Checar se o incidente em questão infringiu dispositivos legais que possam desencadear processos administrativo-disciplinares ou penais;
4. Se a solução não for validada, reencaminhar o chamado para o Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação.

Responsável:

Analista da SSI.

Saída:

- Chamado/ticket validado;

	**Comunicar as partes interessadas**

Objetivo:

Garantir que as informações sejam comunicadas àquele público-alvo que irá se beneficiar delas ou que necessitem agir com base nelas.

Entradas:

Chamado/ticket

Descrição da atividade:

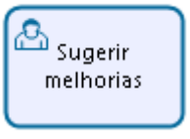
1. Reunir informações sobre o incidente de segurança da informação, principalmente aquelas que identificam as partes afetadas, os ativos afetados, a causa, a solução do incidente e, se possível, a origem do ataque;
2. Comunicar o conteúdo adequado para sua respectiva parte interessada;

Responsável:

Analista da SSI.

Saída:

- Chamado/ticket validado;

	**Sugerir melhorias**

Objetivo:

Emitir recomendações sobre práticas mais comuns de prevenção relacionadas ao incidente em questão, melhorando o Sistema Gestor de Segurança da Informação (SGSI).

Entradas:

- Chamado/ticket;

Descrição da atividade:

1. Analisar criticamente o ciclo de vida do incidente e as informações inseridas no chamado a fim de identificar pontos de melhoria;
2. Registrar informações no chamado para que sejam comunicadas ao final do processo.
3. Encaminhar a sugestão para o ator competente (unidade da CTIC, CGSIC, CGovTIC, Diretoria Geral, Presidência).

Responsáveis:

- Analista da SSI;

Saída:

- Sugestão de melhoria, quando couber.
- Inserção de informação no chamado/ticket.

ANEXO I - Fluxo do Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação