PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
SECRETARIA-GERAL DA PRESIDÊNCIA
COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Institui diretrizes para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta dos Processos Administrativos nº 15452/2020 e nº 14484/2014;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela ENSEC-PJ;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 130/2021, que Institui a Política de Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, assim como o conteúdo das normas de segurança da informação instituídas pelo Tribunal e a ela alinhadas;

CONSIDERANDO as boas práticas para gestão de incidentes de segurança da informação dispostas nos padrões ABNT NBR ISO/IEC 27002 e 27035 e nas medidas de segurança recomendadas pelo *CIS Critical Security Controls* (Controles Críticos de Segurança do *CIS - Center for Internet Security - cisecurity.org*),

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui diretrizes para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional do Trabalho da 18ª Região (TRT18).

Art. 2º Para os fins desta Portaria, consideram-se as seguintes definições:

I – ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

II – ativo: algo que tem valor e necessita ser devidamente protegido;

III – controle: medida que mantém e/ou modifica o risco;

IV – evento de segurança da informação: ocorrência indicando uma possível violação de segurança da informação ou falha de controles;

V – incidente de segurança da informação: um ou vários eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos de uma organização ou comprometer suas operações;

VI – vulnerabilidade: fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças.

Parágrafo único. O Anexo I contextualiza as definições dos incisos de I a VI deste artigo através da representação gráfica do relacionamento entre elas.

Art. 3º A unidade de gestão de segurança da informação revisará anualmente a presente norma, assim como minutará, solicitará aprovação, divulgará, manterá atualizado e testado um Plano de Gestão de Incidentes de Segurança da Informação fundamentado nas diretrizes desta Portaria, observando o alinhamento com outros documentos correlatos, a exemplo dos Planos de Continuidade de Negócios do TRT18 e de Continuidade de Serviços Essenciais de TIC.

CAPÍTULO II
DA FINALIDADE, RELEVÂNCIA E OBJETIVOS

Art. 4º A finalidade da gestão de incidentes de segurança da informação é evitar ou conter o impacto dos incidentes de segurança da informação, a fim de minimizar os danos diretos e indiretos ao TRT18.

Art 5º A abordagem planejada e estruturada de gestão de incidentes de segurança da informação é relevante para reforçar o Sistema de Gestão de Segurança da Informação do TRT18 e visa alcançar os seguintes objetivos específicos:

I – detectar, notificar e avaliar eventos de segurança da informação e decidir se os mesmo são ou não incidentes;

II – responder a incidentes de segurança da informação, incluindo a ativação de controles apropriados para prevenir, reduzir e se recuperar de impactos;

III – relatar vulnerabilidades de segurança da informação, para que possam ser avaliadas e tratadas de forma adequada;

IV – aprender com incidentes e vulnerabilidades de segurança da informação, instituir controles preventivos e fazer melhorias na abordagem geral da gestão de incidentes de segurança da informação.

Parágrafo único. O sucesso da abordagem de gestão de incidentes de segurança da informação depende do trabalho colaborativo de todos os componentes organizacionais.

CAPÍTULO III
DAS DIRETRIZES

Art. 6º Para apoiar a gestão de incidentes de segurança da informação, o TRT18 adotará categorias e classes de incidentes predefinidas pela unidade de gestão de segurança da informação.

Art. 7º O processo global de gestão de incidentes de segurança da informação se dá por meio de atividades organizadas nas fases de “Planejamento e Preparação”, “Detecção e Notificação”, “Avaliação e Decisão”, “Respostas” e “Lições Aprendidas”, conforme o detalhamento que se segue:

I – Planejamento e Preparação, que envolve:

a) elaboração e revisão da presente Portaria;

b) identificação e revisão dos demais regulamentos e documentos relacionados ao tema;

c) elaboração e revisão do Plano de Gestão de Incidentes de Segurança da Informação, que também atenda os requisitos de gestão de incidentes ocorridos em meios físicos ou cibernéticos, assim como os que possam acarretar risco ou dano relevante aos titulares de dados pessoais;

d) estabelecimento de uma ou mais equipes para tratamento e resposta a incidentes de segurança da informação/cibernética;

e) identificação, relacionamento e conexão com entidades internas e externas (ex.: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário - CPTRIC-PJ, Política Federal, Autoridade Nacional de Proteção de Dados Pessoais - ANPD);

f) suporte técnico e organizacional (ex.: definição e implementação de processos de trabalho, ferramentas tecnológicas, equipes de apoio jurídico e administrativo);

g) execução regular de atividades de conscientização da força de trabalho do TRT sobre gestão de incidentes de segurança da informação e inclusão das demandas de treinamento específicas em seu programa de capacitação;

h) teste regular do Plano de Gestão de Incidentes de Segurança da Informação no contexto dos testes do Plano de Continuidade de Negócios do TRT da 18ª Região.

II – Detecção e Notificação, que envolve a detecção, coleta de informações associadas e geração de relatórios sobre ocorrência de eventos e a existência de vulnerabilidades de segurança da informação por meios manuais ou automatizados;

III – Avaliação e Decisão, que envolve a avaliação das informações associadas à ocorrência de eventos e identificação de vulnerabilidades e a decisão de classificar ou não eventos como incidentes de segurança da informação e determinar as ações adequadas de resposta;

IV – Respostas, que envolve a execução de ações determinadas na

fase “avaliação e decisão”, visando prevenir ou conter, erradicar e recuperar dos incidentes de segurança da informação e gerar relatórios sobre os mesmos para uso interno e externo;

V – Lições Aprendidas, que envolve identificar lições com incidentes e vulnerabilidades tratados e o subsequente registro e comunicação dos mesmos com vistas à revisão e melhoria da implementação de controles, da avaliação de riscos, de regulamentos, planos, processos, procedimentos, modelos de relatórios, estrutura e funcionamento de equipes de tratamento e resposta a incidentes, dentre outros.

Parágrafo único. O Anexo II ilustra o fluxo de eventos e incidentes de segurança da informação por meio das fases do processo geral de gestão de incidentes de segurança da informação, suas atividades, principais papéis e tomadas de decisão relacionadas.

Art. 8º Gestores e usuários de sistemas e serviços de informação providos pelo TRT18 devem notificar ao ponto de contato (unidade de atendimento de TIC, por exemplo), o mais breve possível, os eventos e vulnerabilidades de segurança da informação de que tenham conhecimento, orientando-se pelos procedimentos e meios de notificação previamente divulgados.

Parágrafo único. Em conformidade com as orientações e condições indicadas nos respectivos acordos ou contratos, as organizações que fornecem suporte a tais sistemas e serviços, em instalações locais ou em nuvem, deverão notificar o TRT18 sobre possíveis incidentes e vulnerabilidades de segurança da informação de que tenham conhecimento.

Art. 9º Nos casos de suspeita de incidentes de segurança da informação em meio cibernético, a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR do TRT18 atuará em todas as fases do processo de gerenciamento de incidentes.

§1º Incidente relevante ocorrido em meio físico será tratado por equipe de tratamento e resposta a incidente indicada pelo gestor de segurança da informação e instituída pela Presidência, que irá atuar até a sua resolução e encerramento e será apoiada, no que couber, por orientações, práticas e ferramentas disponibilizadas pelo agente responsável pela ETIR.

§2ª Não havendo autorização prévia, as equipes de tratamento e

resposta a incidentes devem solicitar aprovação superior (escalar o incidente para o gestor e este para a Presidência, se necessário) caso uma interrupção ou degradação momentânea de serviço crítico faça parte das estratégias de resposta a um incidente em andamento.

§3º Configurada uma crise, conforme critérios detalhados no Plano de Gestão de Incidentes de Segurança da Informação, o tratamento do incidente passará a ser conduzido pela Equipe de Gestão de Crises do TRT18, instituída pela Presidência em ato próprio, que será apoiada pela ETIR ou pela equipe de tratamento e resposta a incidente de segurança da informação designada, conforme o caso.

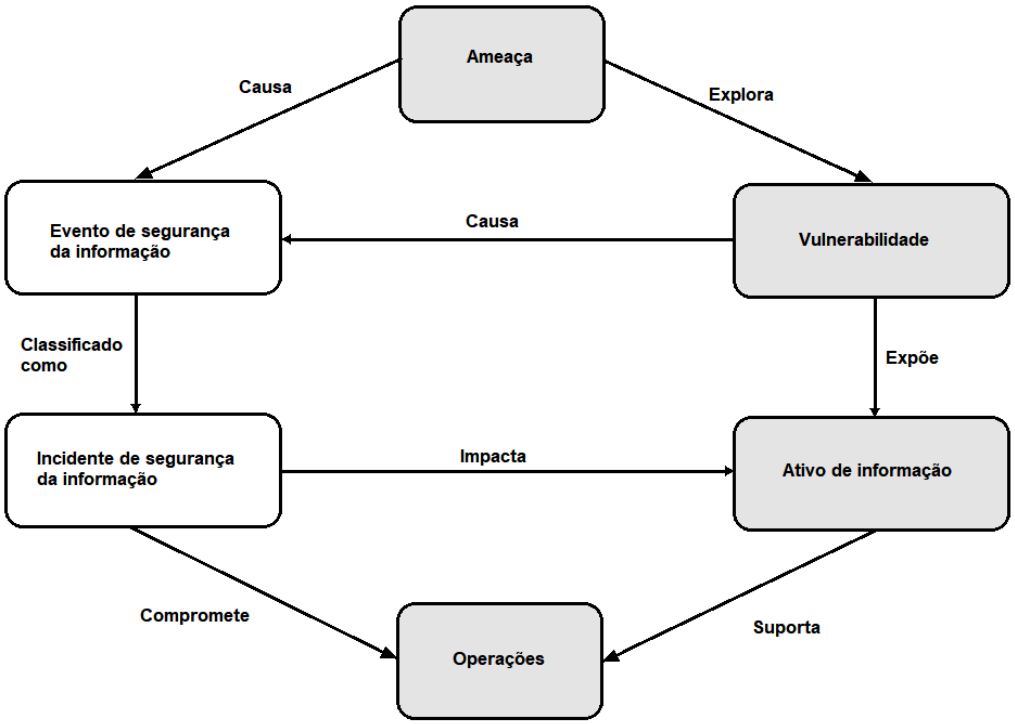
CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 10. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria TRT 18ª GP/SGGOVE nº 1696/2020.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
DANIEL VIANA JÚNIOR
Desembargador-Presidente
TRT da 18ª Região

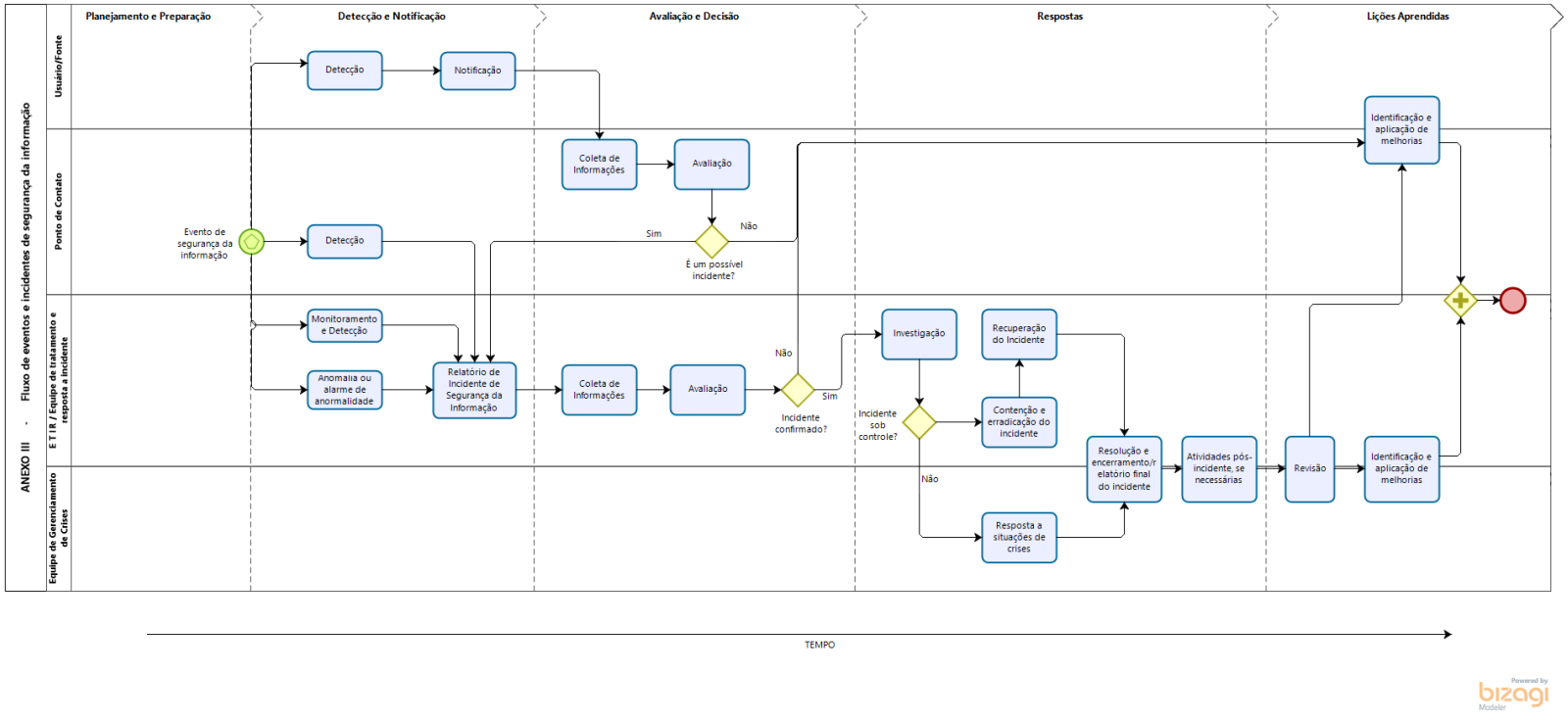
ANEXO I



Os objetos sombreados são pré-existentes e são afetados pelos objetos não sombreados, resultando em um incidente de seguranda da informação.

Fonte: adaptado da ISO/IEC 27035-1:2016

ANEXO II



Fonte: adaptado da ISO/IEC 27035-1:2016

Goiânia, 18 de dezembro de 2022.
[assinado eletronicamente]

DANIEL VIANA JÚNIOR

DESEMB. PRES. DE TRIBUNAL