PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO Nº. 103/2019/GP/TRT 19ª, DE 29 DE OUTUBRO DE 2019

Aprova a Norma de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região.

O DESEMBARGADOR VICE-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO, NO EXERCÍCIO DA PRESIDÊNCIA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas de Governança de TIC que visam garantir a disponibilidade e integridade dos sistemas, aplicativos, dados e de documentos digitais do TRT da 19ª Região;

CONSIDERANDO a inexistência no âmbito do TRT da 19ª Região, de formalização quanto ao processo de gestão de incidentes de segurança da informação, na área de tecnologia da informação;

CONSIDERANDO o disposto no artigo 7º, inciso II, alínea "b", do Ato nº 45/2018 do TRT da 19ª Região, que instituiu a Política de Segurança da Informação;

CONSIDERANDO o disposto no artigo 12, inciso II, alínea "b", da Resolução nº 211/2015 do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO as determinações do Acórdão CSJT-A-1453-83.2015.5.90.0000, relativo à Auditoria na Área de Gestão de Tecnologia da Informação;

RESOLVE:

Art. 1º. – Aprovar a Norma de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região, na forma do Anexo, para observância e aplicação em todo o Regional.

Art. 2º. – Este Ato entrará em vigor a partir da data de sua publicação.

Dê-se ciência, cumpra-se e
Publique-se.

Original assinado
PEDRO INÁCIO DA SILVA
Desembargador do Trabalho, no exercício da Presidência

Publicada no BI nº 10 de 30/10/2019.

ANEXO ÚNICO
NSI002 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

1.1. Disciplinar a criação do Grupo de Respostas a Incidentes de Segurança da Informação (GRISI) no âmbito do Tribunal Regional do Trabalho da 19ª Região (TRT19).

1.2. Estabelecer as diretrizes e definir o Processo de Gestão de Incidentes de Segurança da Informação aplicáveis ao ambiente tecnológico do TRT19.

2. MOTIVAÇÕES

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

2.2. Necessidade de formalização do GRISI e seu funcionamento.

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

2.4. 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.

2.5. 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 13.10.2008, 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 - APF;

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19.08.2010, 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 APF.

3.4. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 8.10.2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da APF.

3.5. 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 do contexto da organização.

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

4. CONCEITOS E DEFINIÇÕES

Para os efeitos deste documento são estabelecidos os seguintes 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. **Central de serviços**: ponto único de contato entre o provedor de Serviço de TIC e os usuários.

4.3. **Grupo de Respostas a Incidentes de Segurança da Informação – GRISI**: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação.

4.4. **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.

4.5. **Evidência**: dados que apoiam a existência ou a veracidade de alguma coisa.

4.6. **Fragilidade**: debilidade de um ativo de informação (do ponto de vista da segurança), ou de um controle, e que pode ser explorada por uma ameaça.

4.7. **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.

4.8. **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.

4.9. **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.

4.10. **Tratamento e resposta a incidentes de segurança da informação**: 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.

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

Outras definições relevantes constam na Política de Segurança da Informação.

5. DIRETRIZES

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

5.2. Estão abrangidos por esta norma os eventos de segurança da informação, confirmados ou suspeitos, que estejam relacionados à segurança de sistemas ou redes computacionais que:

5.2.1. Comprometam o ambiente tecnológico do TRT19, seus ativos, informações e processos de negócio;

5.2.2. Contrariem a Política de Segurança da Informação do TRT19;

5.2.3. Causem a interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades;

5.2.4. Acarretem vulnerabilidades de segurança;

5.2.5. Provoquem a divulgação, alteração ou destruição de informações;

5.2.6. Impliquem em prática de ato definido como crime ou infração administrativa.

5.3. O TRT19 providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

6. GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – GRISI

6.1. O GRISI será composto por servidores da Secretaria de Tecnologia da Informação e Comunicações (Setic), que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes de segurança da informação.

6.2. O GRISI deve coordenar as atividades de tratamento e resposta a incidentes de Segurança da Informação, a fim de contribuir para a garantia da disponibilidade, integridade e confidencialidade das informações.

6.3. O GRISI tem autonomia compartilhada. O grupo recomendará, no mínimo, aos gestores das áreas técnicas envolvidas e à Diretoria da Setic, os procedimentos a serem executados ou as medidas de recuperação durante um ataque e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas). De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida ao Comitê de Segurança da Informação e/ou à Presidência do TRT19. As ações serão sempre definidas em conjunto com as instâncias consultadas.

6.4. O GRISI é composto por servidores da Setic, designados por portaria da própria Secretaria, que indicará o nome dos servidores titulares e substitutos que irão compor o GRISI.

6.5. Para cada uma das posições será designado um suplente.

6.6. Caso necessário, poderão ser convocados outros servidores da Setic e/ou servidores de outras áreas do TRT19 (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar o grupo no desenvolvimento de suas atividades.

7. ATRIBUIÇÕES DO GRISI

7.1. Avaliar fragilidades e eventos de segurança associados, principalmente, aos ativos críticos de TIC;
7.2. Comunicar à unidade responsável pelo Macroprocesso de Segurança da Informação a ocorrência de eventos de segurança para tratamento em tempo hábil.
7.3. Investigar e propor ações de contenção para os incidentes de segurança da informação relacionados aos ativos de tecnologia de informação;
7.4. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;
7.5. Fornecer informações e orientações sobre a ocorrência ou prevenção de incidente de segurança da informação;
7.6. Manter os registros dos incidentes de segurança da informação relacionados aos ativos de tecnologia da informação;
7.7. Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários;
7.8. Recolher evidências o quanto antes após a comunicação de ocorrência de um incidente de segurança da informação;
7.9. Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

8. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.1. 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).
8.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:
8.2.1. Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação;
8.2.2. 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;
8.2.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente;

8.2.4. 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;

8.3. 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.

8.4. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através dos canais disponibilizados pelo TRT19, que os reportarão ao GRISI.

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

8.6. 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.

8.7. As equipes da Setic responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados ao GRISI, para o devido registro e encaminhamento.

8.8. O TRT19 poderá receber notificações externas sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, que deverão ser remetidas ao Escritório de Segurança da Informação, para o devido encaminhamento.

8.9. 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.

8.10. O GRISI deve, em conjunto com as outras áreas da Setic, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.

8.11. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada pelo GRISI ou por pessoal competente e por ela autorizado.

8.12. 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.

8.13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRT19 deverão ser comunicados, para avaliação das providências cabíveis.

8.14. O encerramento do incidente de segurança da informação será realizado pelo Escritório de Segurança da Informação, com comunicação a todas as áreas interessadas, na forma e nos casos definidos pelo referido órgão.

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

8.16. 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, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

8.17. O processo será revisto periodicamente e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência do TRT19, objeto de imediata divulgação na forma do item anterior.

9. ATUALIZAÇÃO DA NORMA

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