	Tribunal Regional do Trabalho da 18ª Região Comitê de Segurança da Informação Secretaria de Tecnologia da Informação e Comunicações Núcleo de Segurança da Informação	Código: **NO06** Revisão: **0.0** Vigência: **Publicação no DEJT** Classificação: **PÚBLICO** Ato normativo: **Portaria TRT 18ª GP/DG**

GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1 OBJETIVO

Assegurar que eventos, incidentes e fragilidades de segurança da informação sejam comunicados e gerenciados de forma consistente e efetiva, permitindo a ação corretiva em tempo hábil e a redução de risco de incidentes futuros.

2 APLICAÇÃO

A presente norma de gerenciamento de incidentes de segurança da informação aplica-se no âmbito do TRT 18ª Região (TRT18).

3 REFERÊNCIA NORMATIVA

3.1 Portaria TRT18 GP/DG nº 76/2014 e anexo "**PO01**", que aprova a Revisão 1.0 das diretrizes da Política de Segurança da Informação e Comunicações do TRT18.

3.2 Portaria TRT18 GP/DG nº 154/2014 e anexo "**DO01**", que aprova o documento de Constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no TRT18.

3.3 Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19/08/2010, que trata da gestão de ETIR e das diretrizes para gerenciamento de incidentes em redes de computadores nos órgãos e entidades da Administração Pública Federal (APF).

3.4 Seção 16 da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação).

4 DEFINIÇÕES

Para efeito desta norma, serão adotadas as definições descritas nesta seção e nos documentos PO01 e DO01.

4.1 Ameaça: causa potencial de um incidente indesejado, que pode resultar em um

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

dano para um sistema ou organização.

4.2 Ativo de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

4.3 Contêineres dos Ativos de Informação: o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

4.4 Controle: forma de gerenciar o risco, incluindo diretrizes, políticas, normas, procedimentos, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

4.5 Custodiante do Ativo de Informação: refere-se a qualquer indivíduo ou unidade da organização que tenha a responsabilidade formal de proteger um ou mais ativos de informação, incluindo o modo como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações informadas pelos proprietários dos ativos de informação.

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 Proprietário do Ativo de Informação: refere-se a parte interessada da unidade da organização, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades:

a) descrever o ativo de informação;
b) definir as exigências de segurança da informação e comunicações do ativo de informação;
c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;
d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento; e
e) indicar os riscos que podem afetar os ativos de informação.

4.8 Risco: combinação entre **probabilidade de um evento** (chance de ocorrer) **e suas consequências** (impacto que causaria se ele acontecesse). Como exemplo: a

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

chance de uma ameaça explorar uma vulnerabilidade e causar um dano a um ativo de informação, às informações ou à Organização.

4.9 Vulnerabilidade: fragilidade.

5 RESPONSABILIDADES

5.1 Chefe da Seção de Suporte e Atendimento

Preparar e orientar o Setor de Atendimento para atuar como ponto de contato entre usuários e unidades da Secretaria de Tecnologia da Informação e Comunicações no que diz respeito a receber e registrar notificações de eventos, incidentes e fragilidades de segurança da informação, assim como para proporcionar o retorno sobre os respectivos tratamentos efetuados.

5.2 Usuários

5.2.1 Notificar ao ponto de contato, o mais breve possível, os eventos, incidentes e fragilidades de segurança da informação de que tenham conhecimento, orientando-se pelos procedimentos de notificação previamente divulgados.

5.2.2 Não testar fragilidades, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou sistemas de informação e resultar em responsabilidade administrativa/legal para o indivíduo que executou o teste.

5.3 Agente Responsável - ETIR

5.3.1 Elaborar, solicitar aprovação da STIC e divulgar a lista com os tipos de incidentes tratados pela ETIR.

5.3.2 Elaborar, solicitar aprovação da STIC e divulgar procedimentos sobre:

a) monitoramento, detecção, análise e notificação de eventos e incidentes de segurança da informação;
b) registro das atividades de gerenciamento de incidentes;
c) manuseio de evidências forenses;
d) avaliação e decisão sobre classificação/reclassificação entre evento e incidente de segurança da informação;
e) resposta a incidentes, incluindo escalonamento, recuperação controlada de um incidente e comunicação às pessoas ou organizações, internas e externas.

5.3.3 Divulgar às partes interessadas os limites de atuação da ETIR, conforme restrições contidas no DO01.

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

5.3.4 Observar a Missão, o Modelo de Implementação, a Estrutura Organizacional e a Autonomia explicitadas no DO01, assim como prestar à Comunidade da ETIR os Serviços nele previstos.

5.3.5 Registrar eventos, incidentes e vulnerabilidades de segurança da informação que sejam detectados automaticamente por ferramentas de monitoramento.

5.3.6 Decidir pela reclassificação de eventos em incidentes de segurança da informação e vice-versa.

5.3.7 Observadas as normas e procedimentos de segurança da informação, iniciar e conduzir as atividades de tratamento e resposta:

a) por convocação do Diretor da STIC;
b) por autorização do Diretor da STIC, caso solicitado pelo Agente Responsável pela ETIR;
c) por conta própria, conforme condições previstas no DO01.

5.3.8 Encaminhar aos responsáveis, para o devido tratamento, os registros de notificações que não se enquadrem no escopo de atuação da ETIR.

5.3.9 Fornecer ao Núcleo de Segurança da Informação os subsídios ao alcance da ETIR que forem solicitados para elaboração de estatísticas, planos e rotinas do SGSI.

5.3.10 Buscar meios formais de colaboração entre a ETIR do TRT18 e o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da APF – CTIR Gov.

5.3.11 Comunicar a ocorrência de incidentes de segurança em redes de computadores ao CTIR Gov, conforme procedimentos por ele definidos, com vistas a permitir que sejam dadas as soluções integradas para a APF, bem como a geração de estatísticas.

5.3.12 Havendo indícios de ilícitos criminais durante o gerenciamento de incidentes de segurança em redes de computadores:

a) acionar as autoridades competentes para a adoção de procedimentos legais necessários;
b) observar procedimentos para a preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo adotado pelo TRT18;
c) priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos referidos na alínea anterior.

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

5.4 Custodiantes e/ou Proprietários de Ativos de Informação

5.4.1 Efetuar a resposta a incidentes de segurança da informação diretamente ou sob coordenação da ETIR.

5.4.2 Providenciar ações de redução de riscos advindas de fragilidades detectadas nos ativos de informação sob custódia ou propriedade, seja diretamente ou sob a coordenação da ETIR.

5.4.3 Registrar, conforme procedimentos previamente divulgados, as ações realizadas durante o tratamento de eventos, incidentes e de vulnerabilidades de segurança da informação.

5.4.4 Disponibilizar à ETIR acesso para monitoramento dos ativos de informação críticos e dos respectivos controles quanto à segurança da informação, observadas as normas de controle de acessos e de classificação da informação.

5.5 Diretor da Secretaria de Tecnologia da Informação

5.5.1 Analisar, aprovar ou recusar a lista de tipos de incidentes de segurança da informação a serem tratados pela ETIR.

5.5.2 Analisar, aprovar ou recusar os procedimentos cuja elaboração seja de responsabilidade da ETIR.

5.5.3 Convocar a ETIR para atuar no tratamento de incidente de segurança da informação de que tome conhecimento e entenda ser crítico para os serviços de TIC do TRT18.

5.5.4 A depender do nível de autonomia da ETIR:

a) autorizar ou negar o pedido de tratamento de determinado incidente ou vulnerabilidade solicitado pelo Agente Responsável pela ETIR;
b) elaborar memorando circular que flexibilize sua atuação, conforme condições expressas no DO01.

5.5.5 Prover recursos necessários e suficientes para o bom funcionamento da ETIR.

5.6 Chefe do Núcleo de Segurança da Informação

5.6.1 Obter, junto à ETIR, informações necessárias para elaborar e manter:

a) plano de conscientização, treinamento e capacitação em segurança da informação;
b) rotinas de medição, monitoramento, auditoria e análise crítica do Sistema de Gestão de Segurança da Informação;
c) estatísticas sobre o gerenciamento de incidentes de segurança da informação no TRT18.

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

5.6.2 Colaborar com a ETIR na divulgação dos serviços, procedimentos e recursos necessários para o gerenciamento de incidentes de segurança da informação no âmbito do TRT18.

6 DISPOSIÇÕES GERAIS

6.1 Os procedimentos a serem elaborados, indicados no item 5.3.2, deverão ser organizados de maneira a compor os serviços listados no DO01.

6.2 Cada serviço será disponibilizado com operacionalidade mínima e deverá evoluir através de revisões periódicas, à medida que houver aumento de maturidade e autonomia da ETIR, assim como da complexidade das demandas.

6.3 A data de entrada em funcionamento, dos serviços da ETIR, não ultrapassará:

a) 31/10/2014 para o Serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, principal serviço a ser prestado pela ETIR;
b) 15/12/2014 para o Serviço de Tratamento de Vulnerabilidades;
c) 13/02/2015 para o Serviço de Tratamento de Artefatos Maliciosos;
d) 15/04/2015 para o Serviço de Detecção de Intrusão;
e) 60 (sessenta) dias corridos da publicação de cada revisão do DO01 que acrescente novos serviços.

6.4 Esta norma deverá ser revisada periodicamente, em intervalos de até um ano.

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449

A S S I N A T U R A S

[Documento assinado eletronicamente por]

ABSAYR GONÇALVES SOUZA

COORDENAD CJ-02

PEDRO AUGUSTO DE CARVALHO GONTIJO

ASSESSOR DIR GERAL CJ-3

MARCOS DOS SANTOS ANTUNES

SECRET GERAL JUD CJ-4

RIVADÁVIA BORGES VIANNA

CHEFE DE NUCLEO FC-6

TÚLIO CÉSAR FERREIRA LUCAS

ASSESSOR CJ-3

HUMBERTO MAGALHÃES AYRES

DIR DE SECRET-CJ-3

Goiânia, 24 de julho de 2014.

Cód. Autenticidade 400028258483

Documento juntado por RIVADÁVIA BORGES VIANNA e protocolado em 24/07/2014 18:03:10h. Protocolo nº 14484/2014. Carimbo Eletrônico Nº 3421449