**RESOLUÇÃO Nº 1066/2018**

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro.

O TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pelo artigo 30, incisos IV e XVII, do Código Eleitoral c/c o artigo 21, inciso XIV, do seu Regimento Interno, CONSIDERANDO o disposto no artigo 9º, da Resolução TRE-RJ nº 1.001, de 18 de dezembro de 2017, que determina a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

CONSIDERANDO a Resolução do Conselho Nacional de Justiça nº 211, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD); e CONSIDERANDO os acórdãos do Tribunal de Contas da União em que aquela corte de contas determina a instituição de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais;

RESOLVE:

## CAPÍTULO I

## DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro, vinculada à Diretoria Geral.

Parágrafo único. A ETIR tem como missão a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais.

Art. 2º Para os efeitos desta Resolução, entende-se por:

I - Ativo de Tecnologia da Informação e Comunicação: item de software ou hardware que contribui para um serviço de TIC do TRE-RJ, seja de propriedade do TRE-RJ ou cedido para utilização pelo mesmo;

II - Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

III - Evento: Considera-se um evento qualquer ocorrência identificada em um sistema ou rede de comunicação.

- Eventos abrangem usuários acessando um compartilhamento de arquivos, um servidor receber uma solicitação de acesso a uma página web, o envio de uma mensagem de e-mail ou um bloqueio de acesso realizado por um equipamento de firewall.
- Eventos adversos são aqueles com consequências negativas como quedas de sistema, sobrecarga de pacotes, acesso não autorizado de privilégios administrativos, acesso não autorizado a dados protegidos e execução de malware;

IV - Firewall: dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, de modo a controlar o acesso aos serviços disponibilizados;

V - Hardware: dispositivos físicos e equipamentos utilizados para o armazenamento, processamento, visualização ou transmissão de informações;

VI - Host: qualquer equipamento ou computador conectado a uma rede de comunicação de dados;

VII - Incidente em segurança da Informação: evento adverso com qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado/inesperado que tenha possibilidade de comprometer as operações do negócio ou ameaçar a segurança da informação. São ressalvados eventos adversos causados por causas naturais, falhas no fornecimento de energia ou similares;

VIII - Log: registro de eventos relevantes num sistema computacional;

IX - Malware - software destinado a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar dano, alteração ou roubo de informações;

X - Software: sequência de instruções preparadas para serem interpretadas por um dispositivo de automação com o objetivo de executar tarefas específicas;

XI - SPAM: termo que designa mensagens de correio eletrônico com fins publicitários sem que tenha ocorrido o consentimento do destinatário para o seu recebimento;

XII - Tecnologia da Informação e Comunicação (TIC): conjunto de ferramentas de suporte a processos institucionais, que conjugam recursos, processos e técnicas computacionais para obter, processar, armazenar, fazer uso e disseminar informações;

XIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## CAPÍTULO II

## DO PÚBLICO ALVO

Art. 3º Todos os usuários da rede de computadores e de sistemas utilizados no âmbito do TRE-RJ poderão comunicar supostos incidentes de segurança da informação nas Redes Computacionais do Tribunal.

Parágrafo único. O registro e o acompanhamento dos incidentes de segurança da informação serão realizados por meio da Central de Serviços de TI.

## CAPÍTULO III

## DO MODELO DE IMPLEMENTAÇÃO E ESTRUTURA ORGANIZACIONAL

Art. 4º A ETIR será formada por membros das equipes de Tecnologia da Informação do próprio Tribunal que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

Art. 5º A ETIR será composta pelos seguintes membros, sob a presidência do primeiro:

I - Secretário de Tecnologia da Informação e respectivo substituto;

II - Coordenador da Coordenadoria de Infraestrutura;

III - Coordenador da Coordenadoria de Sistemas Corporativos;

IV - Chefe de Seção e Assistente da Seção de Produção;

V - Chefe de Seção e Assistente da Seção de Desenvolvimento de Sistemas;

VI - Chefe de Seção e Assistente da Seção de Suporte às Redes Locais;

VII - Chefe de Seção e servidor indicado da Seção de Administração Internet/Intranet;

VIII - Chefe de Seção e servidor indicado da Seção de Administração de Banco de Dados;

§1º O Secretário de Tecnologia da Informação será substituído em suas ausências pelo respectivo substituto eventual.

§2º Os membros da ETIR deverão organizar seus afastamentos de forma que se permaneça, pelo menos, 7 (sete)
componentes em regular execução de suas atividades.

§3º Deverá ser elaborada escala de plantão, nos termos das disposições contidas na Resolução TRE-RJ nº 1.032/2018.

Art. 6º A ETIR poderá trabalhar em colaboração com Centros de Resposta a Incidentes de Segurança da Informação de outras entidades públicas e fornecedores de software, hardware e serviços.

## CAPÍTULO IV

## DA AUTONOMIA DA ETIR

Art. 7º A ETIR possuirá autonomia completa e, durante um incidente de segurança em rede computacional, tomará a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

Parágrafo único. As medidas adotadas deverão ser comunicadas imediatamente à Diretoria-Geral, à Comissão de Segurança da Informação e à Assessoria de Segurança da Informação independentemente do detalhamento previsto no artigo 13 desta Resolução.

## CAPÍTULO V

## DO PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM REDE

Art. 8º O procedimento padronizado para o tratamento de incidentes de segurança em rede compreende as seguintes etapas:

I - Recepção da denúncia ou alerta interno de atividade suspeita;

II - Execução de medidas de contenção imediata do incidente;

III - Coleta e preservação de informações e evidências relativas ao incidente;

IV - Análise das informações e evidências;

V - Notificação dos envolvidos;

VI - Análise crítica e medidas corretivas.

Art. 9º Todos os incidentes de segurança da informação em rede deverão ser registrados e receber uma classificação de severidade/urgência.

§1º A ETIR aceitará, investigará e adotará ações corretivas sobre as denúncias originadas internamente ou oriundas dos seguintes órgãos:

- Tribunal Superior Eleitoral - TSE,
- Centro de Atendimento a Incidentes de Segurança CAIS da Rede Nacional de Pesquisa,
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil CERT-BR,
- CTIR Gov - Centro de Tratamento de Incidentes de Redes do Governo - APF
- e de seus colaboradores sobre atividade suspeita tendo como origem ou destino a rede do TRE-RJ.

§2º Serão investigados os alertas provenientes do monitoramento da rede do TRE-RJ, iniciando o processo de tratamento de incidentes de segurança, quando for observada atividade em desacordo com o comportamento esperado.

§3º Serão aceitas denúncias de pessoas físicas ou entidades públicas ou privadas indicando atividade suspeita relacionada à rede do TRE-RJ, quando devidamente evidenciadas.

§4º Os alertas registrados e as denúncias aceitas serão considerados incidentes de segurança da informação em rede.

§5º A classificação de criticidade/urgência deve ser realizada de acordo com os preceitos definidos no anexo desta norma.

Art. 10. A contenção imediata do incidente se dará por meio de bloqueio de acesso à rede por parte do(s) host(s) envolvido(s).

Art. 11. Serão coletadas e preservadas as informações e evidências sobre as atividades suspeitas através dos logs dos diversos sistemas e serviços disponíveis na rede do TRE-RJ.

Art. 12. Todas as informações e evidências serão analisadas para investigar o host que gerou o incidente denunciado.

§1º A identificação do host compreenderá a determinação do seu endereço IP e endereço MAC da interface de rede, nome, switch e porta de acesso, bem como a localização física do mesmo e o(s) usuário(s) envolvido(s), se possível.

§2º O tipo de atividade que gerou o incidente será determinado pelas informações evidenciadas em logs de serviços.

§3º As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

Art. 13. Para cada incidente será encaminhada notificação por escrito da atividade sob investigação à Assessoria de Segurança da Informação e, se for o caso, à área responsável pelo host sob investigação.

§1º o registro dos incidentes bem como as soluções adotadas deverão ficar registradas para formação de histórico, eventuais consultas, preservação de provas e deverão ser armazenados em repositório próprio, com os devidos controles de acesso.

§2º Cabe ao responsável pelos usuários da máquina alvo de investigação o apoio à determinação da origem da atividade que gerou o incidente de segurança, com sua adequada comprovação.

§3º Como origem pode-se considerar:

I - Atividade realizada pelo usuário;

II - Atividade realizada por terceiro com autorização do usuário;

III - Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

§4º Como evidência da origem da atividade pode-se considerar:

I - Logs de acesso local ou remoto da máquina;

II - Logs de detecção de vírus, spyware, malware etc.;

III - Outras informações que possam identificar claramente a origem da atividade.

Art. 14. Caso a área responsável pelo host investigado informe que o problema foi solucionado, a ETIR avaliará se o incidente foi tratado adequadamente e poderá determinar outras medidas corretivas no host identificado.

§1º Nos casos comprovados de comprometimento de sistemas ou equipamentos, o(s) host(s) envolvido(s) permanecerá(ão) bloqueado(s) até a implantação das medidas corretivas apresentadas.

§2º Nos casos de atividade maliciosa de usuário, este terá seus privilégios de acesso suspensos até a definição das medidas administrativas a serem tomadas pela área responsável.

Art. 15. Denúncias em relação à utilização em desacordo com os preceitos de segurança da informação ou questões de segurança do sistema ou da rede, uso indevido de correio eletrônico, envio de SPAM, violação de direitos autorais ou qualquer atividade em desacordo com esta norma devem ser enviadas ao endereço etir@tre-rj.jus.br com a devida comprovação da atividade.

## CAPÍTULO VI

## DAS DISPOSIÇÕES FINAIS

Art. 16. As unidades vinculadas à STI deverão priorizar o atendimento à ETIR quando instadas a participar no processo de resposta a incidentes de segurança da informação em rede.

Art. 17. Caberá à ETIR elaborar Processo de Tratamento e Resposta a Incidentes em Redes de Computadores no âmbito deste Tribunal, visando receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

Parágrafo único. O Processo de Tratamento e Resposta a Incidentes em Redes de Computadores deverá ser revisado periodicamente, no mínimo a cada dois anos, para adaptação às novas ferramentas e boas práticas.

Art. 18. Esta Resolução entrará em vigor na data de sua publicação.

Sala de Sessões, 29 de agosto de 2018.

Desembargador CARLOS EDUARDO DA FONSECA PASSOS
Presidente

ANEXO

TABELA DE CLASSIFICAÇÃO DE CRITICIDADE/URGÊNCIA

| Nível de criticidade | Nomenclatura | Definição do nível de criticidade | Exemplos típicos de incidente |
|---|---|---|---|
| 1 | Extremamente crítico | Incidentes que afetem sistemas ou informações essenciais com potencial de causar impacto no funcionamento dos serviços ou à imagem da instituição | - Determinação judicial para investigação de incidente de segurança da informação;<br>- Destruição de informações e/ou equipamentos;<br>- Comprometimento de ativo de TIC;<br>- Comprometimento de informação;<br>- Atividade ilegal; |
| 2 | Crítico | Incidentes que afetem sistemas ou informações não essenciais ou com reduzido impacto no funcionamento dos serviços ou à imagem da instituição | - Hacker externo<br>- Hacker interno<br>- Acesso não autorizado<br>- Violações à Política de Segurança da Informação<br>- Uso indevido de ativo de TIC |
| 3 | Não crítico | Possíveis incidentes, incidentes sem potencial de impacto ou incidentes já contidos que envolvam investigação de longo prazo. | - Ataques de Negação de serviços DoS<br>- Vírus / Worm<br>- Email |