ATO TRT5 N. 0041, DE 9 DE MARÇO DE 2021 *

Institui o Comitê de Crises Cibernéticas no Tribunal Regional do Trabalho da 5ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 5ªREGIÃO, DESEMBARGADORA DALILA ANDRADE, no uso de suas atribuições legais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma que ofereça as informações necessárias aos processos deste Tribunal;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação (TI) que visam garantir a disponibilidade e integridade dos ativos tecnológicos do TRT da 5ª Região;

CONSIDERANDO a necessidade de agir de forma proativa e reativa a incidentes de segurança da informação;

CONSIDERANDO que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

CONSIDERANDO a importância de estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes das normas NBR ISO/IEC 27001:2013 e 27002:2013, que tratam da segurança da informação;

CONSIDERANDO a importância de estabelecer objetivos, princípios e diretrizes de Gerenciamento de Crises alinhados às recomendações constantes da norma BS 11200: 2014, que tratam da gestão de crises;

CONSIDERANDO a necessidade de adequação à Resolução n. 360, de 17 de dezembro de 2020; e

CONSIDERANDO o PROAD n. 413/2021,

RESOLVE:

Art. 1º Fica instituído o Comitê de Crises Cibernéticas no Tribunal Regional do Trabalho da 5ª Região.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos deste normativo, são estabelecidos os seguintes conceitos e definições:

I - ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;

II – ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III- atividades críticas: atividades que devem ser executadas para garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

IV - crise: um evento ou série de eventos danosos que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

V – crise cibernética: decorre de incidentes em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

VI – evento: qualquer ocorrência observável em um sistema ou rede de uma organização;

VII – gerenciamento de crise: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas;

VIII – GRIS: Grupo de Resposta a Incidentes de Segurança da Informação, formalizado em ato próprio, responsável pelo gerenciamento e prevenção de incidentes de segurança da informação;

IX – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

X – incidente grave: evento que tenha causado dano, colocado em risco ativo de informação crítico ou interrompido a execução de atividade crítica por um período inferior ao tempo objetivo de recuperação; e

XI – incidente de segurança da informação: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão.

CAPÍTULO II

DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 3º O gerenciamento de incidentes se refere às atividades que devem ser executadas na ocorrência de evento adverso de segurança da informação, para avaliar o problema e determinar a resposta inicial.

Art. 4º O gerenciamento de crise se inicia quando:

I – caracterizado grave dano material ou de imagem;

II – for evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

III – o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

IV – o incidente atrair grande atenção da mídia e da população em geral.

CAPÍTULO III

DA COMPOSIÇÃO DO COMITÊ DE CRISES CIBERNÉTICAS

Art. 5º O Comitê de Crises Cibernéticas terá a seguinte composição:

~~I – Desembargadora Presidente, DALILA ANDRADE;~~

~~II – Desembargador Corregedor Regional, ALCINO BARBOSA DE FELIZOLA SOARES;~~

~~III – Presidente do Comitê de Segurança da Informação, Juiz Gestor Nacional de Metas e Juiz Auxiliar da Presidência, FIRMO FERREIRA LEAL NETO;~~

~~IV – Diretor da Secretaria-Geral da Presidência, MAYSA OLIVEIRA LAGO DOS REIS;~~

~~V – Diretor da Secretaria de Comunicação Social, JOSEMAR ARLEGO JÚNIOR;~~

~~VI – Diretora da Secretaria de Tecnologia da Informação e Comunicações, ÉRICA CRISTINA DÓREA ROSSITER TAVARES;~~

~~VII – Diretor-Geral, TARCÍSIO JOSÉ FILGUEIRAS DOS REIS;~~

~~VIII – Diretor da Secretaria de Assessoramento Jurídico, KARINA MUNIZ MACHADO;~~

~~IX – Diretor da Coordenadoria de Segurança Institucional, FABIANO BARBAGELATA DRUMMOND;~~

~~X – Encarregado de Dados Pessoais; e~~

~~XI – Chefe do Escritório de Segurança da Informação, MARCO ANTÔNIO COSTA SIMÕES.~~

~~*(Incisos I a XI alterados pelo Ato GP nº 0373/2021).*~~

~~*I – Desembargadora Presidente, Débora Machado;*~~

~~*II – Desembargadora Corregedora Regional, Luíza Aparecida Oliveira Lomba;*~~

~~*III – Presidente do Comitê de Segurança da Informação, Juiz Firmo Ferreira Leal Neto;*~~ ~~*(Inciso alterado pelo Ato GP nº 0060/2022).*~~

~~*III - Presidente do Comitê de Segurança da Informação, Juiz André Oliveira Neves;*~~

~~*IV – Secretário-Geral da Presidência, Taciano Barbosa Vasconcelos;*~~

~~*V – Diretor da Secretaria de Comunicação Social, Josemar Arlego Júnior;*~~

~~*VI – Diretora da Secretaria de Tecnologia da Informação e Comunicações, Érica Cristina Dórea Rossiter Tavares;*~~

~~*VII – Diretor-Geral, Orocil Pedreira dos Santos Júnior;*~~

~~*VIII – Diretora da Secretaria de Assessoramento Jurídico, Edite Mesquita Hupsel;*~~

~~*IX – Diretor da Coordenadoria de Segurança Institucional, Fabiano Barbagelata Drummond;*~~

~~*X – Encarregada pelo tratamento de dados pessoais, Juíza Marília Sacramento, Juíza Auxiliar da Presidência; e (Inciso alterado pelo Ato GP nº 0335/2022).*~~

~~*X – Encarregada pelo tratamento de dados pessoais, Juíza Marília Sacramento, Juíza Auxiliar da Presidência;*~~

~~*XI – Chefe do Escritório de Segurança da Informação, Marco Antônio Costa Simões*~~

~~Parágrafo único. A coordenação do Comitê de Crises Cibernéticas ficará a cargo do Presidente do TRT da 5ª Região. *(Inciso alterado pelo Ato GP nº 0335/2022).*~~

~~XI – Chefe do Escritório de Segurança da Informação, Marco Antônio Costa Simões; e *(Inciso alterado pelo Ato GP nº 0281/2023).*~~

~~*XI – Chefe do Escritório de Segurança da Informação,* Hetug Sardeiro Porto;~~

~~XII - Gerente de Projetos Estratégicos em Tecnologia da Informação, Ruth Marques Gomes de Oliveira. *(Inciso inserido pelo Ato GP nº 0335/2022). (Inciso alterado pelo Ato GP nº 0281/2023).*~~

~~XII - Gerente de Projetos Estratégicos em Tecnologia da Informação, Ruth Marques Gomes de Oliveira; e~~

(Incisos I a XII alterados pelo Ato GP nº 0770/2023).

I – Desembargador Presidente, Jéferson Muricy;

II – Desembargadora Corregedora Regional, Ivana Mércio Nilo de Magaldi;

III - Presidente do Comitê de Segurança da Informação e Encarregada pelo Tratamento de Dados Pessoais, Juíza Andrea Presas Rocha;

IV – Secretário-Geral da Presidência, Hélio Eloy Alves Dias Filho;

V – Diretor da Secretaria de Comunicação Social, Josemar Arlego Júnior;

VI – Diretora da Secretaria de Tecnologia da Informação e Comunicações, Érica Cristina Dórea Rossiter Tavares;

VII – Diretor-Geral, Tarcísio Filgueiras;

VIII – Diretora da Secretaria de Assessoramento Jurídico, Edite Mesquita Hupsel;

IX – Diretor da Coordenadoria de Segurança Institucional, Fabiano Barbagelata Drummond;

X - Chefe de Divisão de Processos de Segurança Cibernética, Ruth Marques Gomes de Oliveira;

XI – Diretora da Coordenadoria de Segurança da Informação, Danielle Débora Cerqueira Oliveira; e

XII - Chefe da Divisão Especializada em Segurança Cibernética, Hetug Sardeiro Porto.

~~XIII – Gestora de Segurança da Informação, Danielle Débora Cerqueira Oliveira.~~ *(Inciso excluído pelo Ato GP nº 0770/2023).*

CAPÍTULO IV

DURANTE A CRISE

Art. 6º O Comitê de Crises Cibernéticas deve coordenar ações para garantir que a comunicação entre as áreas envolvidas em crise seja tratada como fator crítico para uma organização responder a uma crise cibernética de longa duração ou de grande impacto.

Art. 7º Assim que o GRIS (Grupo de Resposta a Incidentes de Segurança da Informação) identificar que um incidente constitui crise cibernética, deverá ser reunido imediatamente o Comitê de Crises Cibernéticas.

§ 1º O Comitê de Crises Cibernéticas deve reunir-se presencialmente ou virtualmente, através de tecnologia oficial de videoconferência adotada no Tribunal, para deliberar se o incidente reportado pelo GRIS constitui crise cibernética.

§ 2º Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente, podendo reunir-se a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

§ 3º O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros deste Comitê e a atores eventualmente convidados a participar das reuniões.

§ 4º O Comitê de Crises Cibernéticas deve ter acesso ágil a meios que permitam fazer declarações públicas à imprensa.

§ 5º O Comitê de Crises Cibernéticas deve contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise.

Art. 8º O Comitê de Crise Cibernéticas deverá coordenar esforços com equipes administrativas e técnicas do TRT da 5ª Região para:

I – entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II – levantar todas as informações relevantes, verificando fatos e descartando boatos;

III – levantar soluções alternativas para a crise, apreciando sua viabilidade e suas consequências;

IV – avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

V – centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VI – realizar comunicação tempestiva e eficiente, que evidencie o trabalho diligente das equipes e enfraqueça boatos ou investigações paralelas que alimentem notícias falsas;

VII – definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII – aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

IX – solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X – apoiar equipes de resposta e de recuperação com gerentes de crise experientes;

XI – avaliar a necessidade de recursos adicionais extraordinários para apoiar as equipes de resposta;

XII – fornecer aconselhamento sobre as prioridades e estratégias da organização para uma recuperação rápida e eficaz;

XIII – definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV – elaborar plano de retorno à normalidade.

Art. 9º As etapas e procedimentos de resposta são diferentes de acordo com o tipo de crise e são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 10. Os incidentes graves que ocasionam a deflagração de uma crise cibernética deverão ser comunicados ao Tribunal Superior do Trabalho, Conselho Superior da Justiça do Trabalho e ao Conselho Nacional de Justiça.

CAPÍTULO V

FASE DE APRENDIZADO E REVISÃO (PÓS-CRISE)

Art. 11. Quando as operações retornarem à normalidade, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Art. 12. Para a identificação das lições aprendidas e a elaboração de relatório final, deve ser objeto de avaliação:

I – a identificação e análise da causa do incidente;

II – a linha do tempo das ações realizadas;

III – a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;

IV – os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

V – o escalonamento da crise;

VI – a investigação e preservação de evidências;

VII – a efetividade das ações de contenção;

VIII – a coordenação da crise, liderança das equipes e gerenciamento de informações; e

IX – a tomada de decisão e as estratégias de recuperação.

Art. 13. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta e a melhoria do processo de prevenção de crises cibernéticas.

Art. 14. Deve ser elaborado relatório contendo a descrição e detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

Art. 15. Revogam-se as disposições em contrário.

Art. 16. O presente Ato entra em vigor a partir da data de sua publicação.

DALILA ANDRADE
Desembargadora Presidente

Disponibilizada no DEJT/TRT5-BA. em 09.03.2021, páginas 2-3, com publicação prevista para o 1º dia útil subsequente, nos termos da Lei 11.419/2006 , RA TRT5 33/2007 e o Ato TRT5 GP 10/2021.

**Alterada pelo Ato nº 0373/2021, disponibilizado no DEJT/TRT5-BA, Caderno Administrativo, em 24.11.2021, página 5.*

***Alterado pelo Ato GP nº 0060/2022, disponibilizado no DEJT/TRT5-BA, Caderno Administrativo, em 15.02.2022, página 2.*

*****Alterado pelo Ato GP nº 0281/2023, disponibilizado no DEJT/TRT5-BA, Caderno Administrativo, em 30.05.2023, páginas 1-2.*

Thelma Fernandes, Analista Judiciário – Núcleo de Divulgação – TRT5

******Alterado pelo Ato GP nº 0770/2023, disponibilizado no DEJT/TRT5-BA, Caderno Administrativo, em 1º.12.2023, páginas 2-3.*

Thelma Fernandes – Analista Judiciário
Núcleo de Preservação da Memória Institucional.