PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

ATO GP Nº 01, DE 07 DE JANEIRO DE 2022

Institui a Política de Gerenciamento de Incidentes Cibernéticos no âmbito do Tribunal Regional do Trabalho da 2ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria nº 192, de 27 de julho de 2021, do Conselho Nacional de Justiça, que aprova os Protocolos e Manuais criados pela Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça;

CONSIDERANDO o Ato GP nº 28, 10 de dezembro de 2012, que instituiu a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 2ª Região;

CONSIDERANDO o Ato GP nº 7, de 09 de fevereiro de 2021, que constitui o Comitê de Crises Cibernéticas no âmbito do Tribunal Regional do Trabalho da 2ª Região;

CONSIDERANDO a Portaria GP nº 21, de 08 de abril de 2021, que institui equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética – ETIR no âmbito do Tribunal Regional do Trabalho da 2ª Região,

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Instituir Política de Gerenciamento de Incidentes Cibernéticos no âmbito do Tribunal Regional do Trabalho da 2ª Região.

Art. 2º Esta Política estabelece as atividades necessárias para a implantação dos seguintes protocolos:

I - Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e

III - Protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

Art. 3º Incidente de segurança de Tecnologia da Informação e Comunicações - TIC é qualquer evento, confirmado ou sob suspeita, que:

I - viole a Política de Segurança da Informação do Tribunal Regional do Trabalho da 2ª Região;

II - permita ou facilite acesso não autorizado ao ambiente computacional ou às informações armazenadas digitalmente por este Tribunal;

III - represente ameaça às informações armazenadas, processadas ou trafegadas pelos serviços de TIC;

IV – acarrete exposição de dados e informações confidenciais.

Art. 4º O gerenciamento de incidentes cibernéticos será realizado mediante processo definido e constituído formalmente, contendo, no mínimo, as fases de detecção, registro, análise, tratamento e encerramento dos incidentes de segurança da informação.

Art. 5º Os(as) usuários(as) deverão notificar à Central de Serviços de TIC qualquer incidente de segurança de TIC identificado.

CAPÍTULO II
ADEQUAÇÃO DO AMBIENTE COMPUTACIONAL

Art. 6º Os ativos de informação que compõem o parque tecnológico do Tribunal devem ter seu relógio sincronizado com o serviço de relógio mantido pela Secretaria de Tecnologia da Informação e Comunicações.

§ 1º O serviço de relógio deve oferecer mecanismo de redundância e/ou alta disponibilidade.

§ 2º O serviço de relógio em uso no Tribunal deve utilizar ao menos 3 (três) fontes externas de horário sincronizado, de maneira a garantir a consistência de horário em todo o ambiente computacional.

Art. 7º Ativos de informação são os equipamentos de TIC que processam, armazenam ou manipulam informações no ambiente computacional do TRT2, incluindo *notebooks* corporativos, microcomputadores corporativos e equipamentos servidores.

Art. 8º Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes a segurança da informação, considerando, no mínimo:

I - autenticação, tanto as bem-sucedidas quanto as malsucedidas;

II - acesso a recursos e dados privilegiados;

III - adição ou remoção de contas em grupos com privilégios administrativos;

IV - acesso ou alteração nos registros de auditoria.

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

§ 1º Os registros devem incluir as seguintes informações:

I - identificação inequívoca do(a) usuário(a) que acessou os recursos, quando o acesso for autenticado;

II - natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;

III - data, hora e fuso horário, observando o previsto no Art. 6º;

IV - endereço IP e porta de origem da conexão;

V - identificador do ativo de informação;

VI - coordenadas geográficas, se disponíveis;

VII - qualquer outra informação que auxilie na correta identificação da origem do evento.

§ 2º Quando viável, deve ser registrado o *log* de acesso a URLs realizado por qualquer ativo ou sistema corporativo.

§ 3º Os ativos de informação que não permitem estes registros devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

Art. 9º Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.

Parágrafo único. Os registros de auditoria armazenados remotamente devem ser mantidos por, no mínimo, 5 (cinco) anos, sem prejuízo de outros prazos previstos em normativos específicos. *(Incluído pelo Ato n. 19/GP, de 5 de maio de 2022)*

Art. 9º-A Deverá ser implantada solução analítica de segurança cibernética, que ofereça auxílio para a correlação e análise de registros de auditoria. *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

§ 1º As informações provenientes desta solução devem ser revistas diariamente, com o objetivo de identificar eventos suspeitos com potencial de dano ao ambiente computacional. *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

§ 2º A solução deve ter suas configurações revisadas no mínimo mensalmente, considerando o histórico de informações, as boas práticas, as novas ameaças e as sugestões do fabricante, com o objetivo de identificar e aplicar melhorias necessárias na identificação de eventos suspeitos. *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

§ 3º Devem ser configurados alertas para, no mínimo, as seguintes situações: *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

I - adição ou remoção de contas em grupos com privilégios administrativos; *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

II - *logins* sem sucesso de contas administrativas. *(Incluído pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

CAPÍTULO III
PREVENÇÃO DE INCIDENTES CIBERNÉTICOS

Art. 10. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) deverá coordenar os esforços para promoção da proteção do ambiente computacional do Tribunal por meio da detecção e resposta a incidentes cibernéticos.

Parágrafo único. A ETIR deverá considerar:

I - identificação dos ativos que suportam os serviços críticos do Tribunal. Referidos ativos devem receber foco prioritário:

a. nas ações preventivas;

b. nas ações de monitoramento; ou

c. nas ações de testes.

II - estabelecimento de comunicação e cooperação com outras equipes de tratamento e resposta a incidentes cibernéticos para troca de conhecimento de informações sobre ameaças e ataques reais e aprimoramento contínuo dos controles empregados na defesa do ambiente cibernético do Tribunal Regional do Trabalho da 2ª Região;

III - desenvolvimento e implantação de controles para a proteção de dados e a manutenção dos serviços críticos;

IV - desenvolvimento e implantação de atividades para o monitoramento e detecção de incidentes cibernéticos;

V - desenvolvimento, implantação e manutenção de procedimentos para resposta aos principais tipos de incidentes cibernéticos, considerando sua identificação, contenção e erradicação, além das ações necessárias para a recuperação dos serviços prejudicados em razão destes incidentes;

VI - realização de testes para validação dos controles e procedimentos estabelecidos.

CAPÍTULO IV
CRISES CIBERNÉTICAS

Art. 11. Durante as atividades de análise e tratamento dos incidentes cibernéticos, a ETIR poderá identificar situação de crise.

§ 1º Para a identificação de uma crise a ETIR deverá considerar:

I - caracterização de grave dano material ou de imagem ao TRT2;

II - constatação de que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período;

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

III - impacto do incidente cibernético em atividade-fim ou serviço crítico mantido pelo TRT2;

IV - atenção da mídia e da população em geral.

§ 2º A ETIR comunicará ao Comitê de Crises Cibernéticas, tempestivamente, a ocorrência de qualquer incidente que constituir ou der início a uma crise cibernética.

Art. 12. O Comitê de Crises Cibernéticas se reunirá em sala de situação preparada com os meios necessários para a deliberação com tranquilidade a respeito do ambiente cibernético.

§ 1º A sala de situação deverá atender, preferencialmente, aos seguintes requisitos:

I - deve conter ao menos 1 (um) ramal telefônico;

II - capacidade para, pelo menos, 6 (seis) pessoas;

~~III - pontos de redes e *notebooks* para acesso à internet;~~

III - pontos de redes, além de microcomputadores ou *notebooks* para acesso à internet; *(Redação dada pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

IV - deve conter equipamento com função de impressão e *scanner*;

V - deve conter fragmentadora de papel;

VI - deve ter acesso controlado;

VII - deve se localizar, preferencialmente, próximo a local onde se possa fazer declarações públicas à imprensa.

~~§ 2º Em tempos de pandemia, de distanciamento social, de inexistências de salas disponíveis ou quando for identificada como a maneira mais conveniente para a reunião intempestiva do Comitê de Crises Cibernéticas, será utilizada solução de videoconferência implantada no Tribunal para as deliberações deste Comitê.~~ *(Revogado pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

Art. 13. Ao final de uma situação de crise, será elaborado relatório final de tratamento do incidente cibernético, considerando:

I - Informações sobre a gestão do incidente, como as equipes envolvidas, as decisões tomadas durante o tratamento do incidente cibernético, as ações de contenção e recuperação empregadas, etc;

II - identificação e análise da causa-raiz do incidente cibernético;

III - a linha do tempo das ações realizadas;

IV - impacto identificado nos dados e ambiente computacional;

V - informações a respeito da coleta e preservação das evidências identificadas;

VI - ações objetivas sugeridas para diminuir a probabilidade da ocorrência de incidentes similares ou

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

diminuir o impacto caso eles ocorram;

VII - as oportunidades de melhoria de processo, de tecnologia ou de gestão identificadas.

~~Art. 14. Quando forem identificados incidentes cibernéticos relacionados a dados pessoais, a ETIR deverá comunicar o Comitê Gestor de Proteção de Dados Pessoais.~~

Art. 14. Quando forem identificados incidentes cibernéticos relacionados a dados pessoais, a ETIR deverá comunicar o Comitê de Segurança da Informação e Proteção de Dados Pessoais. *(Redação dada pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

CAPÍTULO V
COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DIGITAIS

Art. 15. A ETIR deverá elaborar e executar procedimentos para a coleta e preservação de evidências digitais, tais como:

I - as mídias de armazenamento envolvidas no incidente cibernético ou suas imagens forenses;

II - os dados voláteis armazenados nos equipamentos, como memória RAM;

III - os *logs* locais e remotos relacionados.

§ 1º As ações de restabelecimento do serviço não devem comprometer a coleta e preservação da integridade das evidências.

§ 2º Quando não for possível a preservação das mídias de armazenamento dos dispositivos afetados em virtude da necessidade do restabelecimento do serviço afetado, a pessoa responsável pela ETIR deverá supervisionar a coleta de todos os dados necessários para a investigação do incidente cibernético, tais como *logs*, arquivos e configurações do sistema operacional, dentre outros, respeitando-se a estrutura e os metadados dos arquivos originais, como data e hora de criação e as permissões vigentes.

§ 3º Na hipótese do 15º § 2º, a pessoa responsável pela ETIR deverá fazer constar em relatório a impossibilidade de preservação das mídias afetadas e listará todos os procedimentos adotados.

§ 4º Para a preservação da integridade das informações, será gerado arquivo com a lista de todos os arquivos coletados e seus respectivos resumos criptográficos (*hashes*). Deverá, também, ser gerado resumo criptográfico do arquivo que contém esta lista.

§ 5º O material coletado será lacrado e custodiado pela pessoa responsável pela ETIR, ou por servidor(a) indicado(a) por ela, e ficará a disposição da Administração ou das autoridades acionadas para a continuidade das investigações.

Art. 16. Quando for identificado incidente penalmente relevante, a ETIR comunicará imediatamente à Administração para o início das tratativas com as autoridades competentes.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.

Art. 17. A Secretaria de Tecnologia da Informação e Comunicações - SETIC elaborará plano de ação para adequação do ambiente computacional considerando, no mínimo, os ativos que suportam os sistemas críticos.

~~Parágrafo único. O plano de ação será aprovado pelo Comitê de Segurança da Informação e Comunicações no prazo máximo de 90 (noventa) dias.~~

Parágrafo único. O plano de ação será aprovado pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais no prazo máximo de 90 (noventa) dias. *(Redação dada pelo Ato n. 10/GP, de 19 de janeiro de 2024)*

Art. 18. Este Ato entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Publique-se e cumpra-se.

São Paulo, data da assinatura eletrônica.

LUIZ ANTONIO M. VIDIGAL
Desembargador Presidente do Tribunal

Fonte: BRASIL. Tribunal Regional do Trabalho (2. Região). Ato GP nº 01, de 07 de janeiro de 2022. Diário Eletrônico da Justiça do Trabalho: Caderno Administrativo [do] Tribunal Regional do Trabalho da 2. Região, São Paulo, n. 3387, p. 2-5, 7 jan. 2022.