PORTARIA TRT/GP/DG Nº 176/2024

Define a Política de Gestão de Incidentes de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições regimentais,

CONSIDERANDO a observância e adoção das recomendações do *framework* de governança de TIC COBIT 5.0;

CONSIDERANDO as normas da família ISO 27000, que tratam da definição de requisitos para um sistema de segurança da informação;

CONSIDERANDO o disposto na Resolução CNJ Nº 370, de 28 de janeiro de 2021;

CONSIDERANDO o disposto na Resolução CNJ Nº 396, de 7 de junho de 2021;

CONSIDERANDO as Recomendações da Portaria CNJ Nº 162, de 10 de junho de 2021;

CONSIDERANDO a Resolução Administrativa Nº 32/2024 que define a Política de Segurança da Informação e atribui à Presidência do Tribunal a responsabilidade da publicação de atos complementares;

CONSIDERANDO a aprovação, pelo Comitê de Segurança da Informação e Proteção de Dados em reunião ordinária de 18 de janeiro de 2024, da proposta de minuta para o presente normativo,

R E S O L V E:

DEFINIR a Política de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 24ª Região, nos termos desta Portaria.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 1º Para fins desta Portaria, considera-se:

I. **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do Tribunal Regional do Trabalho da 24ª Região;

II. **Ameaça:** ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização;

III. **Ativos de TIC:** qualquer mecanismo ou dispositivo de *software* ou *hardware* que compõem a infraestrutura da rede de dados e que é utilizado como ferramenta de trabalho na atividade operacional, tática ou estratégica do TRT da 24ª Região;

IV. **Base de conhecimentos:** conjunto de conhecimentos acumulados a respeito dos incidentes e seus respectivos tratamentos;

V. **Incidente de segurança da informação:** materialização de uma ameaça que provoca danos a um ou mais ativos, além de impactos ao negócio. São exemplos de incidentes de segurança:

a. perda de serviço, equipamentos ou recursos;
b. mau funcionamento ou sobrecarga de sistema;
c. erros humanos;
d. não conformidade com políticas ou diretrizes;
e. violação de procedimentos de segurança física;
f. mudanças descontroladas de sistemas;
g. mau funcionamento de *software* ou *hardware*; ou
h. violação de acesso;

VI. **Usuário de TIC:** todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função

pública em qualquer unidade organizacional do Tribunal, e que para exercer suas atividades se utilizam de um ou mais ativos de TIC;

VII. **Nuvem:** Infraestrutura de tecnologia para armazenamento de dados, serviços, soluções e sistemas, em ambiente externo ao *data center* do TRT da 24ª Região.

CAPÍTULO II
DIRETIRIZES E PRINCÍPIOS CRÍTICOS

Art. 2º A Política de Gestão de Incidentes de Segurança da Informação é parte integrante da Política de Segurança da Informação e terá as seguintes diretrizes e princípios:

I. estabelecer o processo "Gerenciar Incidentes de Segurança da Informação" para detectar, registrar, diagnosticar, responder e solucionar incidentes de segurança da informação;

II. estabelecer, por meio do processo "Gerenciar Incidentes de Segurança da Informação", protocolos para prevenção a incidentes cibernéticos, para o gerenciamento de crises cibernéticas e para a investigação de ilícitos cibernéticos, que sirvam como ferramentas para garantir um sistema de segurança cibernética eficaz e eficiente;

III. oferecer diretrizes que tenham como foco a manutenção e a continuidade dos serviços de TIC, ou o seu restabelecimento em menor tempo possível, e com a priorização esperada pela administração estratégica;

IV. oferecer transparência técnica, administrativa e jurídica na gestão de incidentes de segurança da informação.

Art. 3º O Plano de Comunicação, descrito no Anexo, define os elementos mínimos relacionados à comunicação dos eventos relativos a incidentes de segurança da informação.

CAPÍTULO III

DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTE DE SEGURANÇA CIBERNÉTICA (ETIR)

Art. 4° A Equipe de Tratamento e Resposta a Incidente de Segurança Cibernética (ETIR) terá como missão o planejamento e a execução de ações que ofereçam respostas eficientes aos incidentes de segurança cibernética que apresentem risco à confidencialidade, integridade e disponibilidade dos dados e serviços de TIC do TRT da 24ª Região.

Art. 5° O público-alvo da ETIR é o conjunto de pessoas, unidades, órgãos ou entidades que se utilizam de um ou mais ativos de TIC e são atingidos por um evento que culminou em um incidente de segurança da informação.

Art. 6° A ETIR será composta por:

I. Chefe da Divisão de Proteção de Dados e Segurança da Informação, que exercerá as funções de coordenação da ETIR;

II. Chefe da Divisão de Infraestrutura de TI;

III. Chefe do Núcleo de Sistemas de Informação;

IV. Chefe do Núcleo de Microinformática e Suporte ao Usuário; e

V. Chefe do Setor de Segurança Cibernética.

Art. 7° O modelo de implementação da ETIR foi definido a partir da nomeação de integrantes das unidades técnicas da SETIC, responsáveis pela manutenção e acompanhamento diários dos ativos de TIC que podem ser atingidos por um incidente de segurança da informação.

Art. 8° O monitoramento de incidentes de segurança da informação será realizado pela Divisão de Proteção de Dados e Segurança da Informação, unidade responsável pela coordenação de execução das atividades do processo de trabalho, cujo chefe da unidade acionará os demais integrantes

da ETIR a partir da detecção do alcance do incidente nos ativos de TIC.

Art. 9º A ETIR terá autonomia compartilhada com o Secretário de Tecnologia da Informação e Comunicações para garantir as melhores ações de resposta para um incidente, atendendo às necessidades estratégicas da Administração.

§ 1º A ETIR submeterá as ações de resposta a incidentes de segurança que envolvam impacto aos usuários de serviços de TIC à deliberação do Comitê de Segurança da Informação e Proteção de Dados (CSEGINF) e, em caso de incidentes críticos, aos integrantes do Grupo de Gestão de Crise de Cibernética (GGCC), convocados nos termos do Anexo.

§ 2º Os tratamentos dos incidentes de segurança da informação serão relatados periodicamente ao Comitê de Tecnologia da Informação e Comunicação - CTIC-TRT24.

Art. 10. As divulgações e as comunicações para o público-alvo dos incidentes de segurança da informação seguirão o Plano de Comunicação anexo a esta política.

Art. 11. Os serviços prestados pela ETIR incluirão as seguintes atividades na detecção e tratamento do incidente:

I. monitoramento dos serviços de TIC por meio da atuação dos seus integrantes, no âmbito de cada unidade da SETIC integrante da ETIR;

II. alertar a Divisão de Proteção de Dados e Segurança da Informação dos possíveis casos de incidente, para registro, análise e acompanhamento da solução;

III. alertar as empresas contratadas que sejam responsáveis por suporte técnico em ativos de sua responsabilidade e que estejam envolvidos no incidente, para as providências contratuais;

IV. gestão e monitoramento da execução de procedimento para restauração ou manutenção de serviço após incidente de segurança, no âmbito de cada unidade da SETIC integrante da ETIR;

V. participação em todo o processo de execução de ações e atividades relacionadas ao tratamento do incidente de segurança da informação;

VI. apresentação das soluções possíveis para o Secretário da SETIC, para deliberação compartilhada, e para o CSEGINF, quando envolver decisão estratégica ou negocial para o tratamento do incidente;

VII. abertura de ordem de serviço para as diferentes unidades e técnicos da SETIC para execução de ações e atividades relacionadas ao tratamento de incidentes dos serviços sob sua responsabilidade; e

VIII. apresentar ao público-alvo o alcance do incidente de segurança, o impacto e o tratamento realizado, conforme Plano de Comunicação.

CAPÍTULO IV
DO PROCESSO DE TRABALHO

Art. 12. A Política de Gestão de Incidentes de Segurança da Informação será executada por meio das atividades constantes no Processo "Gerenciar Incidentes de Segurança da Informação", publicado na página de Governança de TIC, opção "Políticas e Processos de Trabalho".

CAPÍTULO V
DOS RESPONSÁVEIS E DAS RESPONSABILIDADES

Art. 13. As responsabilidades sobre a execução das atividades previstas no processo de trabalho "Gerenciar Incidentes de Segurança da Informação" caberão aos seguintes responsáveis:

I. ao Secretário de Tecnologia da Informação e Comunicações caberá a responsabilidade pelas atividades atribuídas ao papel de "Dono do Processo";

II. ao Chefe da Divisão de Proteção de Dados e Segurança da Informação caberá a responsabilidade pelas

atividades atribuídas aos papéis de "Gerente do Processo" e de "Setor de Segurança da Informação";

III. aos integrantes da ETIR e servidores da SETIC indicados pela ETIR para atuarem no tratamento dos incidentes caberá a responsabilidade pelas atividades atribuídas ao papel de "Equipe de Tratamento e Resposta"; e

IV. aos fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem, caberá a responsabilidade por atividades do processo externo denominado "equipe técnica contratada".

CAPÍTULO VI
DO ÂMBITO E DA APLICAÇÃO

Art. 14. A Política de Gestão de Incidentes de Segurança da Informação aplica-se a todos os usuários de TIC do TRT da 24ª Região, nos termos da Política de Segurança da Informação.

CAPÍTULO VI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 15. Ficam revogadas as disposições contrárias a este normativo, notadamente a Portaria TRT/GP/DG Nº 234/2022.

Art. 16. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Proteção de Dados.

Art. 17. Esta Portaria entra em vigor na data de sua publicação.

João Marcelo Balsanelli
Desembargador Presidente

ANEXO

Plano de Comunicação

1. DOS OBJETIVOS DA COMUNICAÇÃO

1.1. O Plano de Comunicação tem como objetivo informar os clientes dos serviços de TI do Tribunal Regional do Trabalho da 24ª Região, internos e externos, por meio de canais pré-estabelecidos.

1.2. Os procedimentos, detalhes técnicos e temporalidade serão definidos de acordo com o tipo da aplicação e descritos no Manual de Execução do Plano de Continuidade, instituído na Política de Gestão de TIC para a Continuidade de Negócios.

2. DO PÚBLICO ALVO

2.1. A comunicação deverá ser direcionada aos públicos interno e externo, de acordo com a conveniência da instituição, observando-se a pertinência para cada tipo de público.

3. DOS RESPONSÁVEIS PELO PROCESSO DE COMUNICAÇÃO

3.1. Em caso de incidente com tratamento e resposta imediato e que não provocou indisponibilidade crítica, ou comprometimento dos dados, a ETIR, por meio dos proprietários dos ativos de TIC, fará as comunicações dos clientes do serviço afetado, a fim de manter transparência e confiabilidade.

3.1.1. O proprietário do ativo de TIC afetado pelo incidente, em negociação com o cliente do serviço, definirá a necessidade de divulgação a usuários do serviço.

3.1.2. A Central de Serviços será comunicada pela ETIR para conhecimento e triagem dos eventuais chamados relacionados ao incidente em questão.

3.2. Para incidentes de segurança críticos, cujo tratamento é abordado pela Política de Gestão de TIC para a Continuidade de Negócios, será convocado o Grupo de Gestão de Crise de Cibernética (GGCC).

3.2.1. O GGCC será composto pelos seguintes integrantes do Tribunal, além dos componentes da ETIR:

3.2.1.1. Desembargador Presidente;

3.2.1.2. Coordenador do CGovTIC;

3.2.1.3. Coordenador do CGRPJE;

3.2.1.4. Coordenador do CSEGINF;

3.2.1.5. Diretor-Geral;

3.2.1.6. Secretário de Tecnologia da Informação e Comunicações;

3.2.1.7. Secretário-Geral Judiciário; e

3.2.1.8. Coordenador da Coordenadoria de Comunicação Social.

3.2.2. O GGCC permanecerá ativo até que os serviços críticos sejam plenamente normalizados e todas as etapas de resposta ao incidente de segurança sejam cumpridas.

3.2.3. O GGCC terá em suas atividades, auxiliado pela ETIR:

3.2.4. avaliar o incidente que gerou a crise para compreender claramente sua gravidade e os impactos negativos.

3.2.5. levantar as informações relevantes com a ETIR e eventuais fornecedores ou colaboradores acionados no atendimento ao incidente para verificar os fatos e descartar boatos.

3.2.6. levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências, para deliberar a solução a ser aplicada.

3.2.7. avaliar a necessidade de suspender serviços e/ou sistemas informatizados para evitar maiores prejuízos durante a crise.

3.2.8. centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas, definindo estratégias de comunicação externa e estabelecendo a mídia mais adequada para se utilizar em cada informação divulgada.

3.2.9. realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas.

3.2.10. aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário – Portaria CNJ Nº 162, de 2021.

3.2.11. solicitar a colaboração de especialistas, de centros de resposta a incidentes de segurança, promovendo intercâmbio com parceiros governamentais ou solicitando à Administração contratações emergenciais, quando necessário.

3.2.12. apoiar equipes de resposta e de recuperação com gerentes de crise experientes.

3.2.13. avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta.

3.2.14. orientar a ETIR sobre as prioridades e estratégias da organização para recuperação rápida e eficaz.

3.2.15. definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente.

3.2.16. elaborar plano de retorno à normalidade.

4. DAS ESTRATÉGIAS DE COMUNICAÇÃO

4.1. A comunicação deverá utilizar meios eletrônicos de envio, com registro do recebimento por parte do destinatário.

4.2. Para incidentes críticos será definido, pelo GGCC, o formato e meio para a comunicação mais rápida e efetiva do público atingido pelo incidente.

5. DOS INSTRUMENTOS DE COMUNICAÇÃO

5.1. Os instrumentos serão, preferencialmente, aqueles disponíveis na infraestrutura da rede do TRT da 24ª Região, na seguinte ordem:

5.1.1. malote digital;

5.1.2. *e-mail* (com opção de recibo);

5.1.3. *broadcast* de rede; e

5.1.4. telefones institucionais.

5.2. De forma complementar, desde que estejam disponíveis, poderão ser utilizados grupos de comunicação fornecidos por redes sociais.

5.3. O GGCC, após a convocação inicial, escolherá o meio de comunicação disponível mais adequado para acelerar as deliberações durante as suas atividades.

6. DA FREQUÊNCIA DA COMUNICAÇÃO

6.1. A comunicação deverá ser realizada sempre que ocorrer qualquer evento que comprometa, total ou parcialmente, a operação dos serviços críticos de TI.

7. DA ELABORAÇÃO DA MENSAGEM

7.1. O conteúdo da mensagem deverá ser objetivo, destacando os seguintes aspectos:

7.1.1. motivo da comunicação;

7.1.2. diagnóstico da situação;

7.1.3. providências tomadas; e

7.1.4. previsão de retorno das operações.