FRANCISCO ROSSAL DE ARAÚJO
24/04/2023 18:44

PORTARIA GP.TRT4 Nº 2.111, DE 20 DE ABRIL DE 2023.

Aprova os Protocolos de Segurança Cibernética do Tribunal Regional da 4ª Região.

O PRESIDENTE DO TRIBUNAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o disposto na Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO o disposto na Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o disposto na Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO o que consta no Processo Administrativo PROAD nº 2379/2021,

RESOLVE:

Art. 1º Aprovar os Protocolos de Segurança Cibernética do Tribunal Regional da 4ª Região, constantes no Anexo Único desta Portaria.

Art. 2º Os Protocolos deverão ser disponibilizados no portal eletrônico deste Tribunal Regional do Trabalho.

Art. 3° Esta Portaria entra em vigor na data de sua publicação.

Documento assinado digitalmente
FRANCISCO ROSSAL ARAÚJO
Presidente do TRT da 4ª Região/RS

PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para a prevenção de incidentes cibernéticos.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

1.3. Promover ações pró-ativas que contribuam para a prevenção de incidentes cibernéticos e também para a resiliência do ambiente tecnológico do Tribunal.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Gerenciamento de Crises Cibernéticas e o Protocolo para Investigação de Ilícitos Cibernéticos.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

2.3. Os atores atuantes ativamente na gestão de segurança cibernética no âmbito do TRT, cujas instituições e atribuições estão definidas na Política de Segurança do TRT (Portaria nº 4772/2008), Regimento Interno e demais portarias relacionadas, são os seguintes:

2.3.1. Comitê Gestor de Segurança da Informação;

2.3.2. Secretaria de Tecnologia da Informação e Comunicações

2.3.3. Escritório de Segurança da Informação;

2.3.4. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;

2.4. Demais atores poderão ser envolvidos em atividades e ações relacionadas à gestão de segurança cibernética como: Presidência, Comitê Permanente de Crises Cibernéticas, Comitê Gestor de Proteção de Dados Pessoais, dentre outros.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. FUNÇÕES DO PROTOCOLO

4.1. Com base na ENSEC-PJ, as funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar.

4.1.1. A função **identificar** consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade. No âmbito do TRT4, a função é contemplada pela seguinte atividade:

4.1.1.1. Gestão de Riscos de Segurança da Informação, formalizada na Política da Segurança da Informação por meio do Anexo 6, e cujo processo foi definido por meio da Portaria 6.137/2014.

4.1.2. A função **proteger** consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados (inclusive pessoais), além de contribuir para a eficiência e eficácia da prestação de serviços. No âmbito do TRT4, a função é contemplada pelas seguintes atividades:

4.1.2.1. Execução contínua do Sistema de Gestão de Segurança da Informação, cujo processo foi instituído por meio da Portaria nº 2.347/2016.

4.1.2.2. Gestão de Continuidade de TIC, formalizada na Política da Segurança da Informação por meio do Anexo 10, e cujo processo foi definido por meio da Portaria 6.137/2014.

4.1.2.3. Gerenciamento da Disponibilidade e Capacidade de TIC, cujo processo foi instituído por meio da Portaria nº 6.969/2017.

4.1.2.4. Processo de Mudança e Liberação de Serviços, instituído por meio da Portaria nº 2.628/2016.

4.1.2.5. Normatização do Uso dos Recursos de TI e controle de acesso, formalizada na Política da Segurança da Informação por meio do Anexo 3.

4.1.2.6. Realização de cópias de segurança do ambiente tecnológico, formalizada na Política da Segurança da Informação por meio do Anexo 4.

4.1.2.7. Implementação de boas práticas de gerenciamento e proteção do ambiente tecnológico, observado normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002 e CIS *Controls*), tais como:

4.1.2.7.1. Gerenciamento de vulnerabilidades;

4.1.2.7.2. Implementação de soluções de segurança do ambiente (firewall, IPS, filtro de conteúdo web, proteção de *endpoint*, detecção e resposta de *endpoint*, dentre outras);

4.1.2.7.3. *Hardening* de serviços e de sistemas;

4.1.2.8. Adequação gradual aos seguintes Manuais de Referência, juntos com a ENSEC-PJ, observando a aplicabilidade de cada

controle ao ambiente e maturidade do TRT4 em relação à segurança cibernética: Proteção de Infraestruturas Críticas de TIC e Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

4.1.3. A função **detectar** consiste no desenvolvimento e aplicação de medidas para identificação de eventos e/ou incidentes de segurança cibernética. A função **responder** consiste na definição e implementação de medidas para responder com eficiência e eficácia a incidentes de segurança cibernética. A função **recuperar** consiste no desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos quando da ocorrência de eventos e/ou incidentes de segurança cibernética. Essas três funções estão contempladas pelas seguintes atividades:

4.1.3.1. Gestão de Incidentes de Segurança da Informação, formalizada na Política da Segurança da Informação por meio do Anexo 8, e cujo processo foi definido por meio da Portaria 7.791/2015.

4.1.3.2. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, formalizada na Política da Segurança da Informação por meio do Anexo 7.

4.1.3.3. Gestão de Continuidade de TIC, formalizada na Política da Segurança da Informação por meio do Anexo 10, e cujo processo foi definido por meio da Portaria 6.137/2014.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.

PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo para Investigação de Ilícitos Cibernéticos.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

2.3. Este protocolo deve ser acionado nos casos em que as medidas estabelecidas no Protocolo de Prevenção de Incidentes Cibernéticos não forem suficientes para evitar a ocorrência de um incidente.

2.4. Para efeitos deste protocolo, são considerados críticos para o funcionamento do Tribunal os seguintes sistemas:

2.4.1. PJe

2.4.2. AUD4

2.4.3. Novajus4

2.4.4. Portal www

2.5. Uma crise cibernética se configura na ocorrência de 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, afetando diretamente ou indiretamente os sistemas críticos do Tribunal.

2.6. Os atores atuantes ativamente no gerenciamento de crises cibernéticas do TRT, cujas instituições e atribuições estão definidas na Política de Segurança do TRT (Portaria nº 4772/2008), Regimento Interno e demais portarias relacionadas, são os seguintes:

2.6.1. Comitê Permanente de Crises Cibernéticas (instituído pela Portaria nº 2.022/2021)

2.6.2. Secretaria de Tecnologia da Informação e Comunicações

2.6.3. Escritório de Segurança da Informação;

2.6.4. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. GERENCIAMENTO DE CRISES CIBERNÉTICAS

4.1. O gerenciamento de crise cibernética se inicia quando:

4.1.1. ficar caracterizado grave dano material ou de imagem;

4.1.2. restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

4.1.3. o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do plano de continuidade de TIC do Tribunal;

4.1.4. atrair grande atenção da mídia e da população em geral; ou;

4.1.5. ocorrer incidente de segurança com dados pessoais;

4.2. Confirmada a crise cibernética, o Comitê Permanente de Crises Cibernética deverá se reunir, observando as definições da Portaria nº 2.022/2021.

4.2.1. Cabe ao Comitê o reporte da crise ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

4.2.2. Caso a crise envolva dados pessoais, o Encarregado de Tratamento de Dados Pessoais do Tribunal deve informar as entidades externas nos termos da LGPD e das demais normativas relacionadas à proteção de dados pessoais vigentes no TRT.

4.3. Para o tratamento do incidente que ocasionou a crise, deverão ser utilizadas políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres e procedimentos técnicos já elaborados e formalizados.

4.4. A crise encerra-se no momento em que for constatado o retorno à normalidade das operações.

4.4.1. Deve ser elaborado um relatório da crise com o intuito de registrar as ações que foram efetivas e as melhorias necessárias para corrigir as causas do incidente que originou a crise (lições aprendidas). O relatório deve conter as seguintes informações:

4.4.1.1. a identificação e análise da causa-raiz do incidente;

4.4.1.2. a linha do tempo das ações realizadas;

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

4.4.1.4. os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

4.4.1.5. as ações realizadas para tratamento da crise e avaliação de sua eficácia.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.

PROTOCOLO PARA INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS

1. OBJETIVOS

1.1. Estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

1.3. Definir requisitos para adequação dos ativos de tecnologia da informação no que tange à configuração e ao registro de informações de auditoria;

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo de Gerenciamento de Crises Cibernéticas.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS EM RELAÇÃO AO REGISTRO DE INFORMAÇÕES

4.1. Os ativos tecnológicos do Tribunal (ex.: estações de trabalho, servidores, serviços, sistemas, dentre outros) devem:

4.1.1. Ser configurados de acordo com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

4.1.2. Ser configurados de forma a registrar eventos relevantes de segurança da informação, bem como de informações que possibilitem a depuração de incidentes e de problemas.

4.1.3. Registrar, sempre que possível, as seguintes informações:

4.1.3.1. identificação inequívoca do usuário que acessou o recurso;

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

4.1.3.3. data, hora e fuso horário, observando-se a HLB; e

4.1.3.4. endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação e demais informações que possibilitem identificar a origem do evento;

4.2. Os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

4.3. O armazenamento dos registros de auditoria deve ser realizado remotamente (e não apenas localmente), por meio do uso de tecnologia aplicável, para, ao menos, os ativos tecnológicos considerados críticos.

5. PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

5.1. Confirmada a ocorrência de um incidente, deve ser avaliada a necessidade de ativação do Protocolo de Gerenciamento de Crises Cibernéticas.

5.2. A investigação do ilícito cibernético deve ser realizada de acordo com as normas estabelecidas na Política de Segurança da Informação vigente, especificamente no tocante ao assunto de gestão de incidentes de

segurança da informação e à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

5.3. Os incidentes de segurança cibernética devem ser registrados em Relatório de Incidente de Segurança da Informação, que contém os dados de identificação de quem o preencheu, data e hora da ocorrência, informações sobre o incidente, como ele foi tratado, oportunidades de melhoria e lições aprendidas.

5.4. Caso seja necessária a coleta de evidências, ela deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.

5.5. Se o incidente de segurança envolver a suspeita de crime, os órgãos competentes devem ser acionados, nos termos da legislação vigente.