Tribunal de Justiça Militar do Estado de Minas Gerais

Diário da Justiça Militar Eletrônico

Nº 116/2023 ANO XIV | Divulgação: sexta-feira, 30 de junho de 2023 | Publicação: segunda-feira, 03 de julho de 2023

Desembargador Rúbio Paulino Coelho, Presidente | Desembargador Fernando A. N. Galvão da Rocha, Vice-Presidente | Desembargador Sócrates Edgard do Anjos, Corregedor | Giovani V. Mendes, Sec.Esp.Presidência

PRESIDÊNCIA

ATO(S) DO PRESIDENTE

PORTARIA N. 1.540, DE 30 DE JUNHO DE 2023

Dispõe sobre a Política de Gestão de Pessoas de Tecnologia da Informação e Comunicação no âmbito do Tribunal de Justiça Militar do Estado de Minas Gerais.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE MINAS GERAIS**, no uso da atribuição que lhe confere o art. 14, inciso VII, do Regimento Interno deste Tribunal,

CONSIDERANDO da Resolução n. 370/2021 do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026, em harmonia com os macrodesafios do Poder Judiciário, em especial com o que estabelece o "Fortalecimento da Estratégia Nacional de TIC e a Proteção de Dados";

CONSIDERANDO da Resolução n. 370/2021 do Conselho Nacional de Justiça, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a necessidade de estabelecer diretrizes e princípios para fundamentar as práticas de gestão de pessoas de TIC neste Tribunal,

RESOLVE:

Art. 1º Fica instituída a Política de Gestão de Pessoas de Tecnologia da Informação e Comunicação no âmbito do Tribunal de Justiça Militar do Estado de Minas Gerais – TJMMG.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 2º Para fins desta Portaria, considera-se:
I - quadro permanente de TIC: conjunto de cargos efetivos cuja especialidade é da área de Tecnologia da Informação e Comunicação;
II - servidores lotados na DIRTIC: todos os servidores que estão efetivamente prestando serviços na Diretoria de Tecnologia da Informação e Comunicação, sejam ocupantes ou não de cargos com especialidade na área de TIC.

CAPÍTULO II
DAS DIRETRIZES E DOS PRINCÍPIOS

Art. 3º A Política de Gestão de Pessoas de TIC possui as seguintes diretrizes:
I - contribuir para o alcance da missão institucional e dos objetivos estratégicos do Tribunal;
II - promover a fixação de servidores no quadro permanente de TIC;
III - propiciar o crescimento profissional dos servidores do quadro de TIC;
IV - valorizar o desempenho dos servidores do quadro de TIC, observados o grau de responsabilidade e as atribuições técnicas específicas;
V - instituir mecanismos de governança a fim de assegurar a aplicação e o acompanhamento dos resultados desta política e do desempenho da gestão de pessoas voltada para a área de TIC.

Art. 4º São princípios da Política de Gestão de Pessoas de TIC:
I - valorização dos servidores do quadro de TIC, de seus conhecimentos, habilidades e atitudes;
II - promoção do bem-estar físico, psicológico, social e organizacional;

III - fomento à cultura orientada a resultados, com foco no aperfeiçoamento dos serviços prestados, assegurando a efetividade da prestação jurisdicional;
IV - desenvolvimento profissional alinhado aos objetivos estratégicos;
V - identificação e promoção de ações de capacitação de pessoas;
VI - estímulo à gestão de talentos, ao trabalho criativo e à inovação;
VII - práticas de gestão de pessoas pautadas na ética, eficiência, isonomia, impessoalidade, publicidade, transparência e no respeito à diversidade;
VIII - fomento à gestão do conhecimento.

CAPÍTULO III
DO QUADRO DE PESSOAL E DA FIXAÇÃO DE SERVIDORES DE TIC

Art. 5º A área de TIC contará com estrutura organizacional e quadro de pessoal específico, composto, preferencialmente, por servidores do quadro permanente do Órgão.
Parágrafo único. O quadro permanente de servidores de TIC deverá ser compatível com a demanda, estabelecendo-se o quantitativo necessário de servidores em função do número de usuários internos e externos de recursos de TIC, atendendo-se, sempre que possível, ao disposto no referencial mínimo estabelecido pelo Conselho Nacional de Justiça.

Art. 6º Os servidores ocupantes de cargos com especialidade na área de Tecnologia da Informação e Comunicação e que fazem parte do quadro permanente do Tribunal deverão ser lotados, prioritariamente, na Diretoria de Tecnologia da Informação.
Parágrafo único. A lotação de servidores do quadro permanente de TIC em unidades que não façam parte da Diretoria de Tecnologia da Informação e Comunicação somente poderá ser autorizada, em caráter excepcional, pelo presidente do Tribunal.

Art. 7º O Comitê de Gestão de TIC realizará, a cada 2 (dois) anos, com o apoio da Diretoria de Recursos Humanos, a análise da rotatividade e evasão de servidores do quadro permanente de TIC, objetivando avaliar a efetividade das medidas adotadas nesta política.

CAPÍTULO IV
DA AVALIAÇÃO DE DESEMPENHO PROFISSIONAL

Art. 8º O desempenho profissional dos servidores da área de TIC, inclusive dos ocupantes em função de confiança que exerçam atividades de TIC, será aferido periodicamente conforme instrumentos de avaliação de desempenho e de cumprimento de metas estipulados pela Diretoria de Tecnologia da Informação e Comunicação e aprovados pela Diretoria de Recursos Humanos.

CAPÍTULO V
DA ESCOLHA DE OCUPANTES DE CARGOS DE CHEFIA E DE ASSESSORAMENTO DE TIC

Art. 9º As funções de confiança e os cargos em comissão da área de TIC deverão ser ocupados, preferencialmente, por servidores do quadro permanente de TIC.

Art. 10. O preenchimento de vagas em funções de confiança decorrentes de vacância ou de aumento de quadro será realizado, preferencialmente, mediante sugestão fundamentada do gestor imediato e aprovação pelo diretor de Tecnologia da Informação, observados a avaliação de desempenho, o perfil profissional e o potencial do servidor.
§ 1º O mérito deve ser fonte primária das indicações para ocupação das funções de confiança e dos cargos em comissão na área de TIC, de forma a maximizar o aproveitamento dos talentos.
§ 2º Para a escolha de líderes ocupantes de funções de coordenação e de gerência na área de TIC, o servidor deverá possuir formação completa de graduação em curso superior na área de Tecnologia da Informação, reconhecida pelo MEC, comprovada por meio de diploma ou certificado de conclusão de curso ou documento equivalente.
§ 3º O critério de que trata o § 2º deste artigo não será aplicável para ocupação da função de coordenação do serviço de Suporte.

CAPÍTULO VI
DOS INCENTIVOS FORMAIS PARA DESENVOLVIMENTO DO PESSOAL DE TIC

Art. 11. O Comitê de Gestão de TIC aprovará o Plano Anual de Capacitação de TIC para o desenvolvimento das competências gerenciais e técnicas necessárias à operacionalização da governança, da gestão e do uso da tecnologia da informação e comunicação.
§ 1º O Plano Anual de Capacitação deverá promover e suportar, de forma contínua, o alinhamento das competências gerenciais e técnicas dos servidores lotados na área de TIC às melhores práticas de governança, de gestão e de atualização tecnológica.

§ 2º A Escola Judicial Militar acompanhará a execução do Plano Anual de Capacitação de TIC, monitorando o alcance dos objetivos, metas e resultados definidos no Plano Diretor de TIC (PDTIC).

Art. 12. Esta Portaria entra em vigor na data de sua publicação.

(a)Desembargador **RÚBIO PAULINO COELHO**
Presidente

PORTARIA N. 1.541, DE 30 DE JUNHO 2023

Institui o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) no âmbito do Tribunal de Justiça Militar de Minas Gerais (TJMMG).

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA MILITAR DE MINAS GERAIS**, no uso da atribuição que lhe confere o art. 14, inciso VII, do Regimento Interno deste Tribunal,

CONSIDERANDO a Resolução n. 396/2021 do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo III da Portaria CNJ n. 162, de 10 de junho de 2021, que constituiu o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

CONSIDERANDO a Resolução CNJ n. 370/2021, que Instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação e Comunicação (TIC), que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

CONSIDERANDO o regramento da Política de Segurança da Informação deste Tribunal de Justiça Militar, estabelecido na Resolução n. 216/2020,

RESOLVE:

Art. 1º Instituir o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) no âmbito do Tribunal de Justiça Militar de Minas Gerais, nos termos desta Portaria.

Art. 2º O Protocolo a que se refere o art. 1º desta Portaria tem por finalidade estabelecer os procedimentos básicos para coletar e preservar evidências, bem como para comunicar fatos penalmente relevantes aos órgãos de investigação e àqueles com competência para o início da persecução penal.

Art. 3º Para os efeitos deste ato normativo, devem ser consideradas as seguintes definições:
I - Ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;
II - Comitê Gestor de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da Justiça Militar do Estado de Minas Gerais (JMEMG);
III - Crise: 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 geradas e que apresentam implicações que afetam uma proporção considerável da organização, bem como seus constituintes;
IV - Crise cibernética: crise que ocorre em decorrência de incidentes em dispositivos, serviços e redes de computadores que causam danos material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
V - ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;
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 - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
IX - Incidente grave: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
X - 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;

XI - Segurança cibernética: é um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares.
XII - Segurança de informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 4º A Diretoria de Tecnologia da Informação e Comunicação (DIRTIC) deverá elaborar um relatório de adequação dos ativos de informação que suportam os serviços essenciais da JMEMG aos requisitos previstos no anexo III da Portaria CNJ n. 162, contendo, no mínimo, as seguintes informações:
I - a situação de cada requisito (atendido, não atendido, atendido parcialmente);
II - a aplicabilidade dos requisitos no ambiente tecnológico do TJMMG;
III - a possibilidade de atendimento e, nessa hipótese, a proposição de prazo de adequação;
IV - a necessidade de capacitação e da aquisição de *softwares* para implementação dos requisitos dos ativos e das práticas de coleta e de preservação de evidências;
V - a possibilidade da adoção de tecnologia que permita a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, a fim de automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.
§ 1º O relatório citado no *caput* deste artigo deverá ser encaminhado ao Comitê Gestor de Segurança da Informação, no prazo de 120 (cento e vinte) dias, contado da publicação deste ato.
§ 2º O mesmo tratamento previsto no *caput* deste artigo deverá ser dispensado aos ativos considerados relevantes, que poderiam ser ponto de entrada para a exploração de falhas, mesmo que não estejam diretamente relacionados à sustentação dos serviços essenciais.

Art. 5º À Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), durante o processo de tratamento do incidente, sem prejuízo de outras ações, compete:
I - conduzir o tratamento do incidente, observando os procedimentos para coleta e preservação das evidências definidos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário, quando constatado ser penalmente relevante;
II - comunicar o fato ao Comitê Gestor de Segurança da Informação;
III - comunicar o fato ao(à) encarregado(a) pelo tratamento de dados pessoais do TJMMG, quando o incidente envolver dados pessoais.
§ 1º O(a) encarregado(a) pelo tratamento de dados pessoais do TJMMG deverá comunicar o incidente aos titulares de dados pessoais que tiverem seus dados vazados e, se entender necessário, à Agência Nacional de Proteção de Dados Pessoais (ANPD).
§ 2º O Comitê de Crise deverá ser sempre acionado quando o incidente for considerado como crise cibernética.

Art. 6º A Presidência encaminhará ao Ministério Público e à Polícia Judiciária toda comunicação de segurança cibernética que seja considerada como possível ilícito criminal.

Art. 7º As ações de coleta e preservação de evidências devem observar o disposto no anexo III da Portaria CNJ n. 162/2021.

Art. 8º As normas estabelecidas nesta Portaria serão revistas anualmente ou, quando necessário, em menor prazo.

Art. 9º Esta Portaria entra em vigor na data de sua publicação.

(a)Desembargador **RÚBIO PAULINO COELHO**
Presidente

PORTARIA N. 1.542, DE 30 DE JUNHO DE 2023

Institui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), no âmbito do Tribunal de Justiça Militar de Minas Gerais.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA MILITAR DE MINAS GERAIS**, no uso da atribuição que lhe confere o art. 14, inciso VII, do Regimento Interno deste Tribunal,

CONSIDERANDO a Resolução n. 396/2021 do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo I da Portaria CNJ n. 162, de 10 de junho de 2021, que contém o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

CONSIDERANDO a Resolução CNJ n. 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação e Comunicação (TIC), que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

CONSIDERANDO o regramento da Política de Segurança da Informação deste Tribunal, estabelecida pela Resolução n. 216/2020,

RESOLVE:

Art. 1º Ficam instituídos, no âmbito do Tribunal de Justiça Militar de Minas Gerais (TJMMG), o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), nos termos dispostos nesta Portaria.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 2º O Protocolo de Prevenção de Incidentes Cibernéticos do TJMMG tem como objetivo:
I - prevenir incidentes cibernéticos por meio das funções identificar, proteger, detectar, responder e recuperar;
II - disciplinar o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do Tribunal de Justiça Militar de Minas Gerais;
III - promover alinhamento às normas, regulamentações e melhores práticas relacionadas à Gestão de Incidentes de Segurança da Informação;
IV - promover ações que contribuam para a resiliência dos serviços de Tecnologia da Informação a ataques cibernéticos.

Art. 3º Para os efeitos deste ato normativo, devem ser consideradas as seguintes definições:
I - Ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;
II - CGTIC: Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação;
III - Comitê Gestor de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da Justiça Militar do Estado de Minas Gerais (JMEMG).
IV- Controle: providência que modifica o risco em qualquer processo, política, dispositivo, prática ou ação;
V - ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;
VI - 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;
VII - PPINC-PJ: refere-se ao Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário definido pelo CNJ, que contempla conjunto de diretrizes para a prevenção de incidentes cibernéticos em seu mais alto nível;
VIII - Resiliência: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente;
IX - Segurança cibernética: é um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares.
X - Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 4º Para implementação do disposto nesta Portaria, deverão ser observados pelas áreas envolvidas os princípios críticos definidos no PPINC-PJ, que são:
I - uso de base de conhecimento de defesa;
II - priorização da segurança da informação;
III - definição e estabelecimento de métricas;
IV - diagnóstico contínuo;
V - formação e capacitação;
VI - busca de soluções automatizadas de segurança cibernética;
VII - resiliência.

CAPÍTULO II
DA COMPETÊNCIA DE ATUAÇÃO

Art. 5º Cabe à Presidência:

I - analisar as deliberações do Comitê Gestor de Segurança da Informação (CSI) sobre gestão de incidentes de segurança da informação e decidir sobre possíveis providências;
II - formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação;
III - comunicar a ocorrência de incidentes penalmente relevantes ao órgão de polícia judiciária competente para apurar os fatos;
IV - acionar o Comitê de Crises Cibernéticas, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, quando necessário.

Art. 6º Cabe ao Comitê Gestor de Segurança da Informação:
I - deliberar sobre as principais diretrizes e temas relacionados à gestão de incidentes de segurança da Informação;
II - monitorar e avaliar periodicamente a estrutura de gestão de incidentes de segurança da informação e o sistema de controles internos, assim como propor melhorias consideradas necessárias;
III - aprovar formalmente o Processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;
IV - deliberar sobre ações de contenção ou prevenção de incidentes de segurança da informação;
V - manifestar-se sobre matérias atinentes à segurança da informação que lhe sejam submetidas;
VI - assessorar, em matérias correlatas, a Presidência do TJMMG.

Art. 7º Cabe ao Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação (CGTIC) assegurar a implementação das ações e dos controles definidos para prevenção de contenção de incidentes de segurança da informação dos ativos do TJMMG.

Art. 8º Cabe à Coordenação de Infraestrutura da DIRTIC:
I - coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à ETIR;
II - garantir que os incidentes de segurança na rede do TJMMG sejam devidamente tratados;
III - adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação na rede interna de computadores sejam informados dos procedimentos adotados;
IV - disseminar cultura voltada para a comunicação de incidentes de segurança da informação;
V - subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança da informação;
VI - desenvolver, testar e implementar um Processo de Gestão de Incidentes de Segurança da Informação e garantir sua efetividade.

Art. 9º A ETIR tem a responsabilidade de receber, analisar, classificar, tratar e responder as notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Art. 10. O funcionamento da ETIR do TJMMG – definição de missão, público-alvo, modelo de implementação, nível de autonomia, integrantes, canais de comunicação de incidentes e os serviços a serem prestados – está regulamentado no anexo único desta Portaria.

CAPÍTULO III
DAS FUNÇÕES DO PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

Art. 11. São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos, conforme definição do PPINC-PJ, identificar e detectar incidentes, responder às demandas deles provenientes, proteger e recuperar a informação.

Seção I
Da Função Identificar

Art. 12. A função “Identificar” consiste na análise dos riscos de ataques cibernéticos a que sistemas, pessoas, dados, recursos e ativos de TI em geral estão expostos, incluindo a elaboração e a execução de um plano de tratamento dos riscos.

Art. 13. A função “Identificar” é executada dentro do escopo do processo de gestão de riscos de segurança da informação, instituído no Tribunal.

Seção II
Da Função Proteger

Art. 14. A função “Proteger” consiste no desenvolvimento e na implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, ativos de informação, bem como a prestação de serviços.
§ 1º A função "Proteger" deve ser implementada pelo conjunto mínimo de ações elencadas a seguir:
I - implantação e aprimoramento contínuo de um Sistema de Gestão de Segurança da Informação (SGSI) no TJMMG;

II - controle de acesso e de utilização de recursos de TI;
III - cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos;
IV - plano de continuidade de TI dos serviços essenciais;
V - gestão de capacidade e disponibilidade de TI dos serviços essenciais;
VI - processo de gerenciamento de mudanças para todos os ativos de TI;
VII - gestão de vulnerabilidades técnicas dos serviços essenciais;
VIII - utilização de ferramenta de segurança para estações de trabalho, contendo, no mínimo, as funções de antivírus, automação de políticas de segurança de *endpoint*, proteção contra criptografia (*ransomware*), controle de aplicativos e de dispositivos removíveis;
IX - controle de acesso a conteúdo na Internet (filtragem *web*);
X - utilização de ferramenta de segurança de rede *next generation firewall;*
XI - uso de antivírus de rede, sistema de detecção e prevenção de ameaças e implementação de redes privadas virtuais (VPN);
XII - integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (serviços essenciais, em detrimento de ambientes de laboratório/desenvolvimento/homologação);
XIII - promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;
XIV - atualização tecnológica constante;
XV - implementação gradual dos controles de segurança da informação presentes na Norma NBR 27002;
XVI - implementação gradual dos controles mínimos recomendados no Manual de Referência para Proteção de Infraestruturas Críticas de TIC, editado pelo Conselho Nacional de Justiça, considerando a escala de aplicabilidade de cada controle em relação ao porte e maturidade do TJMMG em segurança da informação;
XVII - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TJMMG em segurança da informação;
XVIII - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Gestão de Identidade e de Controle de Acesso, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TJMMG em segurança da informação;
XIX - implantação de uma Política de Educação e Cultura em Segurança Cibernética, conforme o anexo VII da Portaria CNJ n. 162, de 10 de junho de 2021.
§ 2º As salvaguardas elencadas no § 1º deste artigo devem ser implementadas para todos os ativos de TIC, no que couber, considerados essenciais ou não ao negócio, permitindo variar quanto ao nível de implementação, de acordo com a natureza e criticidade do ativo.
§ 3º As atualizações dos ativos de TIC (pacotes de segurança, *firmware*, entre outros) devem ser aplicadas, sempre que possível, tão logo liberadas, mas considerando:
I - os riscos decorrentes da atualização;
II - os riscos decorrentes da não aplicação (ou postergação);
III - a criticidade do ativo;
IV - a estabilidade dos serviços.

Seção III

Das Funções Detectar, Responder e Recuperar

Art. 15. As atividades decorrentes das funções "detectar", "responder" e "recuperar" do Protocolo de Prevenção de Incidentes Cibernéticos devem estar cobertas pelo Processo de Gestão de Incidentes de Segurança da Informação.

Art. 16. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá, ainda, ser seguido o Protocolo de Investigação para Ilícitos Cibernéticos.
Parágrafo único. Na ocorrência da hipótese prevista no *caput* deste artigo, o Comitê Gestor de Segurança da Informação e a Presidência do TJMMG deverão ser comunicados.

Art. 17. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e os demais registros restritos aos envolvidos na investigação.

Art. 18. A gestão de incidentes de segurança cibernética deve ser realizada por meio do Processo de Gestão de Incidentes de Segurança da Informação, contendo as fases de detecção, triagem, análise e respostas aos incidentes de segurança.

Art. 19. As ações relacionadas à prevenção de incidentes devem observar, ainda, o disposto no anexo I da Portaria CNJ n. 162, de 2021.

Art. 20. As normas estabelecidas nesta Portaria serão revistas anualmente ou, quando necessário, em menor prazo.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

(a)Desembargador **RÚBIO PAULINO COELHO**
Presidente

ANEXO ÚNICO

1. OBJETIVO
Analisar as notificações e atividades relacionadas a incidentes de segurança da informação em ambiente tecnológico, respondendo às demandas delas provenientes.

2. MISSÃO
Planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do TJMMG.

3. PÚBLICO-ALVO
Usuários do ambiente tecnológico do TJMMG.

4. MODELO DE IMPLEMENTAÇÃO
4.1 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) adotará o Modelo 1 de implementação proposto pelo subitem 7.1 da Norma Complementar n. 05/IN01/DSIC/GSIPR, utilizando a equipe de TI.

4.2 A ETIR será formada por membros lotados na Diretoria de Tecnologia da Informação e Comunicação (DIRTIC), que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

4.3 As funções e os serviços de tratamento de incidente deverão ser realizados, preferencialmente, por administradores de rede ou de sistema, ou, ainda, por peritos em segurança.

4.4 Com base nesse modelo, a Equipe desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém, que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades de maneira pró-ativa.

5. ESTRUTURA ORGANIZACIONAL
5.1 A ETIR será formada por dois integrantes, sendo um deles o Administrador de Redes do TJMMG, que terá a função de Agente Responsável.
5.2 Ao Agente Responsável caberá criar os procedimentos internos, treinar os integrantes, gerenciar as atividades, distribuir tarefas para a equipe, inclusive as de caráter proativo.
5.3 Seus integrantes serão indicados pelo(a) diretor(a) da DIRTIC e designados por meio de portaria.
5.4 Será indicado e designado um suplente para substituir os integrantes quando necessário.
5.5 A ETIR funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação primordialmente reativa e não exclusiva.
5.6 As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos gestores de seus respectivos integrantes.

6. AUTONOMIA DA ETIR
A ETIR-TJMMG tem autonomia compartilhada, ou seja, participará do resultado da decisão, recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão na hipótese de as recomendações não serem seguidas.

7. CANAL DE COMUNICAÇÃO
A comunicação dos incidentes de segurança em rede de computadores à ETIR será feita:
- por e-mail: etir@tjmmg.jus.br;
- por meio de correspondências oficiais (memorandos, ofícios);
- pessoalmente, em casos emergenciais;
- por meio de ferramental tecnológico, no caso de eventos detectados pelo monitoramento da ETIR.

8. SERVIÇOS
8.1 A ETIR prestará os seguintes serviços:
8.1.1 Tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar e classificar as solicitações e alertas e realizar as análises dos incidentes de segurança, procurando

extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.
8.1.2 Tratamento de artefatos maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, ele deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou, pelo menos, sugerida, uma estratégia de detecção, remoção e defesa.
8.1.3 Tratamento de vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, em *hardware* ou em *software*, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.
8.1.4 Emissão de alertas e advertências: serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.

9. DISPOSIÇÕES GERAIS
Este documento deverá ser revisado periodicamente, em intervalos de até dois anos.

PORTARIA N. 1.543, DE 30 DE JUNHO DE 2023

Institui o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) no âmbito do Tribunal de Justiça Militar de Minas Gerais

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA MILITAR DE MINAS GERAIS**, no uso da atribuição que lhe confere o art. 14, inciso VII, do Regimento Interno deste Tribunal,

CONSIDERANDO a Resolução n. 396/2021 do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo II da Portaria CNJ n. 162, de 10 de junho de 2021, que constituiu o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ);

CONSIDERANDO a Resolução CNJ n. 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação (TIC), que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

CONSIDERANDO o regramento da Política de Segurança da Informação deste Tribunal de Justiça Militar de Minas Gerais, estabelecida pela Resolução n. 216/2020,

RESOLVE:

Art. 1º Fica instituído o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC PJ) no âmbito do Tribunal de Justiça Militar de Minas Gerais, nos termos deste ato.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 2º O Protocolo de Gerenciamento de Crises Cibernéticas é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.

Art. 3º Para os efeitos deste ato normativo, devem ser consideradas as seguintes definições:
I - CGTIC: Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação;
II - Comitê Gestor de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da JMEMG;
III - 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 geradas e que apresentam implicações que afetam uma proporção considerável da organização, bem como seus constituintes;

IV - Crise cibernética: crise que ocorre em decorrência de incidentes em dispositivos, serviços e redes de computadores que causam danos material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
V - ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;
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 - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
IX - Incidente grave: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
X - 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;
XI - Segurança cibernética: é um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares.
XII - Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 4º São serviços de Tecnologia da Informação e Comunicação considerados críticos ao funcionamento do Tribunal, para efeito do protocolo a que se refere esta Portaria, os Serviços Essenciais assim definidos pelo Comitê de Governança e Gestão de Tecnologia da Informação (CGTIC) e homologados pelo presidente do TJMMG.

CAPÍTULO II
DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 5º 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. 6º O gerenciamento de crise se inicia quando:
I - restar caracterizado grave dano material ou de imagem;
II - ficar evidenciada a possibilidade de que as ações de resposta ao incidente cibernético persistirão por longo período;
III - 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 TJMMG;
IV - o incidente atrair grande atenção da mídia e da população em geral;
V - ocorrer vazamento de quantidade significativa de dados pessoais.

CAPÍTULO III
DA COMPOSIÇÃO DO COMITÊ DE CRISES CIBERNÉTICAS

Art. 7º Fica instituído o Comitê de Crises Cibernéticas, para cumprimento das competências definidas neste Protocolo de Gerenciamento de Crises, com a seguinte formação:
I - presidente do Tribunal de Justiça Militar;
II - corregedor da Justiça Militar;
III - presidente do Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação (CGTIC);
IV - presidente do Comitê Gestor de Segurança da Informação;
V - chefe do Centro de Segurança Institucional;
VI - encarregado(a) de tratamento de dados no âmbito do TJMMG;
VII - chefe de Gabinete da Presidência;
VIII - secretário(a) especial da Presidência;
IX - diretor(a) de Tecnologia da Informação e Comunicação;
X - diretor(a) judiciário;
XI - diretor(a) administrativo;
XII - diretor(a) de Gestão de Pessoas;
XIII - gerente da Corregedoria;
XIV - coordenador(a) de Infraestrutura e Redes da DIRTIC.
Parágrafo único. O Comitê de Crises Cibernéticas será presidido pelo presidente do Tribunal de Justiça Militar de Minas Gerais e, na sua impossibilidade, será sucedido na ordem dos incisos deste artigo.

CAPÍTULO IV
DOS PROCEDIMENTOS DURANTE A CRISE

Art. 8º Caberá à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), identificando que o incidente de segurança constitui uma crise cibernética, comunicar o fato ao Comitê de Crises Cibernéticas,

que deverá se reunir imediatamente.
§1º Fica definida como sala de situação, para deliberação sobre o incidente que constitui a crise cibernética, a sala de reuniões localizada no 5º andar do edifício-sede da Justiça Militar, local em que será gerida a crise.
§2º Na impossibilidade de a reunião acontecer de forma presencial, poderá ocorrer virtualmente, por meio de solução oficial de videoconferência adotada pelo TJMMG, conforme deliberação do presidente.
§3º 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.
§4º O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros do Comitê e a pessoas eventualmente convidadas.
§5º O Comitê de Crises Cibernéticas deve ter acesso ágil a meios que permitam fazer declarações públicas à imprensa.
§6º O Comitê de Crises Cibernéticas deve contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise.
§7º Os planos de contingências existentes, caso aplicáveis, devem ser efetivados imediatamente após a declaração da crise cibernética, visando à continuidade dos serviços prestados.
§8º A sala de situação deve dispor dos meios necessários como sistemas de áudio, vídeo, chamadas telefônicas, e estar próxima a um local onde se possam fazer declarações públicas à imprensa.

Art. 9º Para eficácia do trabalho do Comitê de Crise, é necessário que os esforços visem:
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 uma comunicação tempestiva e eficiente de forma a evidenciar o trabalho diligente das equipes e a enfraquecer 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;
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;
XIV - elaborar plano de retorno à normalidade.

Art. 10. As etapas e os procedimentos de resposta são diferentes a depender do tipo de crise, sendo necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 11. A Presidência do TJMMG encaminhará comunicado da ocorrência do incidente grave, quando constatada uma crise cibernética:
I - ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça;
II - ao Ministério Público do Estado de Minas Gerais (MPMG), à Defensoria Pública, à Ordem dos Advogados do Brasil, Seção Minas Gerais (OAB/MG) e à Advocacia-Geral do Estado, quando o incidente envolver a prestação jurisdicional.

Art. 12. Cabe ao encarregado(a) de tratamento de dados pessoais comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais a ocorrência de incidente grave, envolvendo dados pessoais, que possa acarretar risco ou dano relevante aos titulares.

Art. 13. Cabe ao(à) diretor(a) de Tecnologia da Informação e Comunicação:
I - identificar e manter documentação técnica atualizada dos ativos de informação que suportam os serviços essenciais;
II - avaliar e tratar os riscos de TIC aos quais as atividades estratégicas estão expostas e que possam impactar diretamente na continuidade do negócio, de acordo com o processo de gestão de riscos de segurança da informação;
III - elaborar um plano de gestão de incidentes cibernéticos para os ativos críticos, o qual deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos; a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente; e a severidade do incidente;

IV - elaborar e testar planos de contingência de TIC para os serviços essenciais, sem prejuízo das ações decorrentes da norma complementar que estabelece as diretrizes para a gestão da continuidade de TIC do TJMMG.

Art. 14. Cabe ao coordenador de Infraestrutura o papel de Agente Responsável pela ETIR, competindo a ele comunicar a ocorrência de incidentes de segurança ao Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (Cert.br).

CAPÍTULO V
DOS PROCEDIMENTOS DURANTE A FASE DE APRENDIZADO E REVISÃO (PÓS-CRISE)

Art. 15. 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. 16. 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;
IX - a tomada de decisão e as estratégias de recuperação.

Art. 17. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (*playbook*) e para a melhoria do processo de preparação para crises cibernéticas.

Art. 18. Deve ser elaborado relatório contendo a descrição e o 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. 19. As ações de resposta e recuperação da crise cibernética devem observar, ainda, o disposto no anexo II da Portaria CNJ n. 162, de 2021.

Art. 20. As normas estabelecidas nesta portaria serão revistas anualmente ou, quando necessário, em menor prazo.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

(a)Desembargador **RÚBIO PAULINO COELHO**
Presidente

Credenciamento de instituição consignatária para efeito de consignação facultativa junto ao Tribunal de Justiça Militar de Minas Gerais
Credenciado: Banco Bradesco S.A.– CNPJ 60.746.948/0001-12
Processo SEI: 23.0.000001073-1
Fundamento: Resolução TJMMG n. 200/2018 e Portaria TJMMG n. 1.111/2018
Período: 2 (dois) anos
Deferimento: 30 de junho de 2023

Deferindo:
- O gozo de 15 (quinze) dias de férias-prêmio, referentes ao 1º (primeiro) quinquênio, a partir de 17/07/2023, requerido pelo servidor Leonardo Henrique Vaz de Melo, JME 0371-9, nos termos da Portaria TJMMG n. 966/2017.

DIÁRIAS DE VIAGEM

Beneficiário: James Ferreira Santos
Cargo: Desembargador
Matrícula: JME-0372-7
Destino: Salvador/BA
Atividade: Participação na 1ª Jornada de Direito Militar UNICORP/TJBA, ENAJUM/STM, EJMSP/TJMSP, EJMRS/TJMRS, EJMMG/TJMMG.
Período de afastamento: 31/08/2023 a 02/09/2023
Concessão de 2,5 (duas e meia) diárias, nos termos da Portaria nº 541/2011.

Beneficiário: Giovanne Gomes da Silva
Cargo: Chefe de Gabinete
Matrícula: JME-0956-7
Destino: Salvador/BA
Atividade: Participação na 1ª Jornada de Direito Militar UNICORP/TJBA, ENAJUM/STM, EJMSP/TJMSP, EJMRS/TJMRS, EJMMG/TJMMG.
Período de afastamento: 31/08/2023 a 02/09/2023
Concessão de 2,5 (duas e meia) diárias, nos termos da Portaria nº 541/2011.

ATO(S) DO VICE-PRESIDENTE

DIÁRIAS DE VIAGEM

Beneficiário: Rúbio Paulino Coelho
Cargo: Desembargador
Matrícula: JME-0276-3
Destino: Salvador/BA
Atividade: Participação na 1ª Jornada de Direito Militar UNICORP/TJBA, ENAJUM/STM, EJMSP/TJMSP, EJMRS/TJMRS, EJMMG/TJMMG.
Período de afastamento: 31/08/2023 a 02/09/2023
Concessão de 2,5 (duas e meia) diárias, nos termos da Portaria nº 541/2011.

SECRETARIA ESPECIAL DA PRESIDÊNCIA

ATO(S) DO SECRETÁRIO

Deferindo, nos termos do art. 33 da Portaria TJMMG n. 908/2016, licenças-saúde aos seguintes servidores:
- Thiago de Morais Coelho, Oficial Judiciário, JME 0998-1,1 (um) dia, em 25/05/2023;
- Letícia Alves de Toledo, Oficial Judiciária, JME 0983-4, 1 (um) dia, em 21/06/2023.

GERÊNCIA ADMINISTRATIVA

AVISO DE LICITAÇÃO

A Gerência Administrativa do Tribunal de Justiça Militar do Estado de Minas Gerais torna público aos interessados do ramo pertinente que irá promover a licitação na forma seguinte:

PREGÃO ELETRÔNICO Nº 12/2023
PROCESSO LICITATÓRIO Nº 10/2023
PROCESSO DE COMPRA SIAD Nº 42/2023

MENOR PREÇO GLOBAL

OBJETO: Contratação de empresa especializada para execução do projeto luminotécnico para a fachada do edifício do Tribunal de Justiça Militar de Minas Gerais, pelo regime de empreitada por preço global, lote único, incluindo todos os serviços necessários, com fornecimento de materiais, mão de obra, equipamentos e ferramentas, além de acabamentos e da limpeza e retirada de entulho e sobras decorrentes dos serviços, conforme especificações técnicas, detalhamentos e condições que serão relacionadas neste Termo de Referência, nos projetos que deram origem aos dados nele inseridos, memoriais descritivos, documentos anexos, e demais disposições deste EDITAL.

Abertura da sessão do Pregão Eletrônico: dia 13/07/2023 às 10:00min (dez horas), por meio do site www.compras.mg.gov.br.

O encaminhamento das propostas deverá ser efetuado por meio do site www.compras.mg.gov.br até a data e horário marcados para abertura da sessão.

O Edital encontra-se à disposição nos sites www.tjmmg.jus.br, link “Licitações” e www.compras.mg.gov.br. Demais informações pelo telefone (31) 3274-1566 ou e-mail: licitacao@tjmmg.jus.br.

JUSTIÇA MILITAR DE PRIMEIRA INSTÂNCIA

AVISO: a partir do dia **15 de maio de 2018**, toda comunicação à Fazenda Pública para a prática de ato processual, inclusive a própria citação, será feita exclusivamente de forma eletrônica.

ÍNDICE POR ADVOGADOS

145316MG => 1; 159247MG => 1; 184705MG => 1;

TERCEIRA AUDITORIA JUDICIÁRIA MILITAR ESTADUAL

MATÉRIA CRIMINAL

1 - 0000285-70.2017.9.13.0003
Réu: Jose Renato Bazelenitz Pinheiro => Reitere-se vista à Defesa Técnica acerca da manifestação do Ministério Público às folhas 449 dos autos. Adv.: Jorge Vieira da Rocha, Jorge Vieira da Rocha Junior, Matheus Gomes da Costa.