da Promotoria de Justiça Criminal de São Mateus, e 2ª Vara Criminal - execução penal, no dia 04/08/2014.

PORTARIA Nº 4.472 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XIV e art. 55,§ 1º, da Lei Complementar 95, de 28/01/1997, o Promotor de Justiça, LÉLIO MARCARINI, para exercer também a função de 1º Promotor de Justiça da Promotoria de Justiça Criminal de São Mateus, e 2ª Vara Criminal - execução penal, no dia 06/08/2014.

PORTARIA Nº 4.473 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XIV e art. 55,§ 1º, da Lei Complementar 95, de 28/01/1997, o Promotor de Justiça, RICARDO ALVES KOKOT, para exercer também a função de 8º Promotor de Justiça da Promotoria de Justiça Cível de Colatina, (somente nas audiências), no dia 30/07/2014.

PORTARIA Nº 4.474 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XIV e art. 55,§ 1º, da Lei Complementar 95, de 28/01/1997, o Promotor de Justiça, RICHARD SANTOS DE BARROS, para exercer também a função de 2º Promotor de Justiça da Promotoria de Justiça de Itapemirim, no período de 12/08/2014 a 22/08/2014.

PORTARIA Nº 4.475 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XIV e art. 55,§ 1º, da Lei Complementar 95, de 28/01/1997, o Promotor de Justiça, SANDRO BARBOSA SGRANCIO, para exercer também a função de 1º Promotor de Justiça da Promotoria de Justiça da Infância e Juventude de Vila Velha, (somente nas audiências), no dia 07/08/2014.

PORTARIA Nº 4.476 de 30 de Julho de 2014
REVOGAR a Portaria nº 471, publicada no Diário Oficial de 25/01/2013, que designa o Promotor de Justiça, JONACI SILVA HEREDIA, para funcionar também nos autos do processo nº 0011195-58.2011.8.08.0014, em curso perante o 1º Promotor de Justiça Criminal de Colatina, a partir de 21/05/2014.

PORTARIA Nº 4.477 de 30 de Julho de 2014
REVOGAR, a partir de 20/05/2014, a Portaria nº 1.032, publicada no Diário Oficial de 26/02/2013, que concedeu ao Promotor de Justiça SÉRGIO GERALDO DALLA BERNARDINA SEIDEL, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97.

PORTARIA Nº 4.478 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XXV, da Lei Complementar Nº 95, de 28/01/1997, o Promotor de Justiça ELION VARGAS TEIXEIRA, para exercer a função de Promotor de Justiça Chefe da Promotoria de Justiça de Muniz Freire, no período de 09/01/2014 a 08/01/2015, conforme Procedimento MP/Nº 32615/2014.

PORTARIA Nº 4.479 de 30 de Julho de 2014
DESIGNAR, na forma do art. 10, inciso XXV, da Lei Complementar Nº 95, de 28/01/1997, o Promotor de Justiça FERNANDO JOSÉ LIRA DE ALMEIDA, para exercer a função de Promotor de Justiça Chefe da Promotoria de Justiça da Infância e Juventude de Cariacica, no período de 02 a 03/07/2014 e no período de 14 a 18/07/2014, conforme Procedimento MP/Nº 32401/2014.

PORTARIA Nº 4.480 de 30 de Julho de 2014
CONCEDER licença para tratamento de saúde ao Promotor de Justiça DANILO RAPOSO LIRIO, no dia 25/07/2014, conforme art. 93, inciso I da Lei Complementar Estadual nº 95/97 e Procedimento MP/Nº 32807/2014.

PORTARIA Nº 4.481 de 30 de Julho de 2014
CONCEDER ao Promotor de Justiça AMÉRICO JOSÉ DOS REIS, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97, a partir de 01/07/2014, conforme Procedimento MP/Nº 32612/2014.

PORTARIA Nº 4.482 de 30 de Julho de 2014
CONCEDER ao Promotor de Justiça ANTONIO CARLOS GOMES DA SILVA JÚNIOR, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97, no período de 07 a 23/07/2014, conforme Procedimento MP/Nº 32451/2014.

PORTARIA Nº 4.483 de 30 de Julho de 2014
CONCEDER ao Promotor de Justiça CLEBER TADEU TÓTOLA, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97, no dia 24/07/2014, conforme Procedimento MP/Nº 32409/2014.

PORTARIA Nº 4.484 de 30 de Julho de 2014
CONCEDER ao Promotor de Justiça FELIPE PACÍFICO DE OLIVEIRA MARTINS, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97, no período de 07 a 23/07/2014, conforme Procedimento MP/Nº 32408/2014.

PORTARIA Nº 4.485 de 30 de Julho de 2014
CONCEDER ao Promotor de Justiça FERNANDO JOSÉ LIRA DE ALMEIDA, a gratificação de função prevista no art. 92, inciso II, alínea "g" da Lei Complementar nº 95/97, no período de 07 a 11/07/2014, conforme Procedimento MP/Nº 32400/2014.

Vitória, 30 de julho de 2014.
EDER PONTES DA SILVA
PROCURADOR-GERAL DE JUSTIÇA

PORTARIA Nº 4.486 de 30 de Julho de 2014
REVOGAR, a partir de 01/08/2014, a Portaria nº 1.250, publicada no Diário Oficial de 06/03/2013, que designou o servidor EDUARDO AGUIAR DE SOUZA, ocupante do cargo efetivo de Agente de Apoio/Função: Administrativo, com lotação na Promotoria de Justiça de Venda Nova do Imigrante, para exercer a função gratificada I, em conformidade com a Lei nº 9.496, publicada no Diário Oficial de 22/07/2010, conforme Procedimento MP/Nº 29765/2014.

PORTARIA Nº 4.487 de 30 de Julho de 2014
DESIGNAR o servidor RAFAEL RIBEIRO BUGARELLI, ocupante do cargo efetivo de Agente de Promotoria/Função: Assessoria, com lotação na Promotoria de Justiça de Venda Nova do Imigrante, para exercer a função gratificada I, em conformidade com a Lei nº 9.496, publicada no Diário Oficial de 22/07/2010, a partir de 01/08/2014, conforme Procedimento MP/Nº 29765/2014.

Vitória, 30 de julho de 2014.
EDER PONTES DA SILVA
PROCURADOR-GERAL DE JUSTIÇA

PORTARIA Nº 4.488 de 30 de julho de 2014

Institui a Política de Segurança da Informação, na área de Tecnologia da Informação, do Ministério Público do Estado do Espírito Santo

O PROCURADOR-GERAL DE JUSTIÇA, no uso das atribuições que lhe são conferidas pelos incisos VII e XII do art. 10 da Lei Complementar Estadual nº 95/1997, e

CONSIDERANDO que a informação é um ativo essencial, o qual necessita de adequada proteção aos vários tipos de ameaças externas e internas que possam comprometer a integridade, confidencialidade e disponibilidade das informações do Ministério Público do Estado do Estado do Espírito Santo ou que estejam sob sua responsabilidade;

CONSIDERANDO a necessidade de implementar um conjunto de controles, normas, procedimentos, padrões e sistemas que visem ao estabelecimento, à implantação, ao monitoramento, à análise e ao melhoramento contínuo da segurança da informação na área de tecnologia da informação;

CONSIDERANDO a crescente importância e o reconhecimento da segurança da informação, que suscita a perquirição por um ambiente seguro, a melhoria dos processos de trabalho, a adoção de novas tecnologias e, sobretudo, a conscientização e a educação das pessoas;

CONSIDERANDO que, conforme disposto no artigo 14, inciso I, da Portaria CNMP-PRESI n° 70, de 27 de março de 2014, é competência do Fórum Nacional de Gestão, por meio de seus Comitês e Grupos de Trabalho, fomentar a uniformização e a padronização da atuação dos diversos ramos e unidades do Ministério Público brasileiro, respeitadas as suas autonomias administrativa, financeira e orçamentária;

CONSIDERANDO que o Comitê de Políticas de Tecnologia da Informação do Ministério Público - CPTI-MP tem por objetivo promover o direcionamento tecnológico do Ministério Público brasileiro, por meio de deliberações que promovam a uniformização, padronização e integração de infraestrutura, sistemas, taxonomia, estatística e governança de tecnologia da informação;

CONSIDERANDO, por fim, a elaboração do Caderno de Boas Práticas em Segurança da Informação pelo Grupo de Trabalho em Infraestrutura, vinculado ao Comitê de Políticas de Tecnologia da Informação do Ministério Público - CPTI-MP, que traz uma série de recomendações no intuito de implantar uma política uniforme nos Ministérios Públicos;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação do Ministério Público do Estado do Espírito Santo, com a finalidade de estabelecer diretrizes de segurança da informação na área de tecnologia da informação, visando à adoção de procedimentos e de mecanismos relacionados à proteção das informações de sua propriedade e sob sua guarda, a serem cumpridos por seus membros, servidores, estagiários e prestadores de serviço.

Art. 2º Para efeito do disposto nesta portaria, considera-se:

I - ameaça: ação, espontânea ou proposital, que afete um sistema por meio de suas vulnerabilidades, causando prejuízos e/ou redução de disponibilidade;
II - ativos de tecnologia da informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação, bem como conexões com a internet, hardware e software;
III - auditoria: análise crítica do sistema de gestão de segurança da informação, verificando a conformidade e a eficácia dos controles implementados;
IV - backup: cópia de segurança gerada para possibilitar o acesso e a recuperação futura das informações;
V - confidencialidade: proteção das informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação;
VI - continuidade do negócio: capacidade estratégica e tática da instituição de se planejar e responder a incidentes e interrupções das atividades de tecnologia da informação, a fim de manter suas operações em um nível aceitável e previamente definido;
VII - controle: qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco, podendo ser de natureza administrativa, técnica, legal ou de gestão;
VIII - disponibilidade: garantir que o serviço esteja funcionando conforme especificado e o acesso às informações esteja disponível somente a usuários autorizados;
IX - firewall: sistema de segurança de computadores usado para restringir o acesso "de/para" em uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas;
X - gestão de risco: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos;
XI- hardware: parte física dos equipamentos tecnológicos, ou seja, conjunto de aparatos eletrônicos, peças e equipamentos;
XII - incidente de segurança da informação: representado por um ou mais eventos de segurança da informação que tenham uma grande probabilidade de comprometer as operações de tecnologia da informação e ameaçar a segurança da informação;
XIII - integridade: toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada;
XIV - proprietário da informação: todo aquele responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes ao órgão ou sob a sua guarda;
XV - segurança da informação: conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio e a diminuição de riscos;
XVI - software: manipulação, instrução de execução, redirecionamento e execução de atividades lógicas dos equipamentos de tecnologia da informação;
XVII - terceiro: qualquer parceiro, fornecedor ou prestador de serviço que acesse informações ou utilize recursos de tecnologia da informação, disponibilizados pelo Ministério Público do Estado do Espírito Santo;
XVIII - usuário: qualquer colaborador seja ele membro, servidor, estagiário, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa ou utiliza informações custodiadas ou de propriedade do Ministério Público do Estado do Espírito Santo;
XIX - vulnerabilidade: fragilidade de um software, sistema operacional ou outro componente da infraestrutura de tecnologia da informação, que pode ser explorada por uma ou mais ameaças.

Art. 3º São diretrizes básicas da Política de Segurança da Informação do Ministério Público do Estado do Espírito Santo:
I - responsabilidade pela garantia da segurança, do controle e da administração das suas informações;
II - informação produzida ou recebida é de propriedade do Ministério Público, devendo ser armazenada e protegida quanto ao seu acesso e uso e classificada quanto à integridade, confidencialidade e disponibilidade;
III - acesso às informações de propriedade do Ministério Público será direcionado ao desempenho das atividades ministeriais e plenamente adequado aos objetivos institucionais;
IV - responsabilidade dos membros, servidores, estagiários e prestadores de serviço do Ministério Público pelo cumprimento da Política de Segurança da Informação;
V - alinhamento das normas, procedimentos e planos de implantação, gestão e auditoria de segurança da informação institucional com a Política de Segurança da Informação;
VI - divulgação ampla e irrestrita da Política de Segurança da Informação;
VII - vedação do uso de informações de propriedade do Ministério Público para interesses que não estejam de acordo com os objetivos institucionais;
VIII - responsabilidade pela realização e pelo acompanhamento das manutenções preventivas periódicas dos equipamentos e instalações, visando à preservação do patrimônio institucional;
IX - manutenção, atualização e supervisão do ambiente tecnológico, de modo a atender os níveis e requisitos de segurança próprios e inerentes às funções institucionais;
X - definição de responsabilidades e de sanções nos casos de violação da Política de Segurança da Informação, para membros, servidores, estagiários e prestadores de serviço do Ministério Público.

Art. 4º São diretrizes relativas ao ambiente e acesso físico, na área de tecnologia da informação:
I - desenvolvimento de planos específicos que englobem a plena conservação do ambiente físico do Ministério Público;
II - controle do acesso físico às dependências e instalações do Ministério Público, disciplinando a circulação de pessoas, materiais e equipamentos;
III - proteção física e adequada dos recursos e instalações críticas ou sensíveis contra os riscos identificados, acessos não autorizados, danos ou interferências, por meio de barreiras de segurança e controles de acesso;
IV - acesso aos painéis de controle e cabeamentos de energia e de comunicações restritos aos técnicos e profissionais das áreas de segurança e de infraestrutura;
V - registro e atualização sistemáticos, em período definido em norma específica, do inventário do conjunto de ativos relevantes, sensíveis e críticos para a instituição;
VI - localização não identificável publicamente das instalações sensíveis e críticas;
VII - exigência de autorização formal para executar intervenções e manutenções no ambiente físico do Ministério Público, as quais deverão estar submetidas a uma supervisão previamente responsabilizada;
VIII - exigência de áreas de limite (perímetro) de segurança para todas as instalações de tecnologia da informação do Ministério Público;
IX - exigência de instalações apropriadas para guarda, utilização e lotação dos recursos tecnológicos e materiais;
X - exigência de instalações e equipamentos adequados à integridade de membros, servidores, estagiários e prestadores de serviço;
XI - estabelecimento de normas e procedimentos para triagem de documentos, em qualquer suporte, antes de seu descarte, reciclagem ou reutilização;
XII - exigência de equipamentos apropriados e pessoal treinado para o combate a incêndio, compatível com a área, espaço físico e instalação a ser protegida;
XIII - utilização de equipamentos de combate a incêndio, quando necessário, de acordo com treinamentos e seguindo instruções do fabricante.

Art. 5º São diretrizes relativas à segurança de tecnologia da informação em recursos humanos:
I - obediência aos dispositivos legais para a seleção, nomeação e contratação de profissionais, considerando as competências de caráter pessoal, profissional e acadêmico;
II - responsabilização dos profissionais de nível hierárquico superior pela supervisão da conduta e do comportamento de seus subordinados diretos e indiretos, identificando as ocorrências que possam comprometer a segurança da informação;
III - compromisso de confidencialidade e de cumprimento da política, das normas e dos procedimentos de segurança da informação do Ministério Público, com previsão de sanções e penalidades em caso de violação das regras;
IV - divulgação ampla entre membros, servidores, estagiários e prestadores de serviço do Ministério Público das medidas e dos procedimentos que eliminem riscos de acessos não autorizados, perdas, danos e violações de segurança com relação aos ativos de tecnologia da informação da instituição;
V - obrigatoriedade do porte e uso de identificação funcional durante a permanência de servidores, estagiários e prestadores de serviço nas dependências, instalações e unidades do Ministério Público;
VI - identificação de membros, servidores, estagiários, prestadores de serviço e visitantes, a qual é imprescindível, pessoal e intransferível, responsabilizando-os pelas ações praticadas por meio dela;
VII - treinamento e atualização sistemática de membros, servidores, estagiários e prestadores de serviço do Ministério Público sobre políticas, normas e procedimentos de segurança da informação, visando ao pleno exercício de suas funções;
VIII - responsabilidade pessoal e intransferível pelo sigilo, privacidade e uso de senhas de acesso aos recursos computacionais, as quais não podem ser compartilhadas, divulgadas, anotadas em papel ou em sistema visível ou de acesso não protegido;
IX - troca imediata de senhas, nos casos de perda, ou mesmo na hipótese de suspeita da quebra de seu sigilo;
X - bloqueio imediato dos acessos aos recursos tecnológicos como perfil de usuário, nos casos de exoneração, aposentadoria, disponibilidade punitiva e desligamentos de qualquer natureza;
XI - previsão formal e contratual de cuidados e responsabilização quanto à segurança dos ativos do Ministério Público nas contratações de prestação de serviços;
XII - uso pessoal da senha, a qual deve ser mantida em sigilo, não permitindo que terceiros a utilizem para o desempenho de qualquer tipo de atividade;
XIII - uso e aplicação da prática de mesa limpa e tela de computador protegida;
XIV - adoção da prática de exclusão de informações críticas e sensíveis das lixeiras;

XV - utilização de sistemas e aplicativos após treinamento operacional específico, seguindo definições e procedimentos registrados em manuais ou documentos similares;
XVI - acompanhamento de toda e qualquer manutenção preventiva e corretiva realizada em equipamentos sob sua responsabilidade;
XVII - obrigatoriedade da ciência e do conhecimento de todo material referente à segurança da informação, disponibilizado pelo Ministério Público;
XVIII - tratamento de documentos adequado e compatível com seu grau de sigilo;
XIX - capacitação e desenvolvimento da equipe de tecnologia da informação em segurança da informação;
XX - conscientização dos membros, servidores, estagiários e prestadores de serviço do Ministério Público quanto às ameaças externas (vírus, interceptação de mensagens e dados, grampos e fraudes e tentativas que ensejam o roubo de senhas) que possam afetar ou ameaçar a segurança das informações da instituição;
XXI - adoção da prática de não abordagem e não discussão em ambientes públicos e áreas expostas de assuntos relacionados ao trabalho;
XXII - esclarecimento imediato das dúvidas relacionadas à política, normas e procedimentos de segurança da informação, com os devidos conhecimento e registro;
XXIII - vedação a membro, servidor, estagiário e prestador de serviço do Ministério Público de:
a) conectar, na rede do Ministério Público, equipamentos não autorizados;
b) alterar nomes padronizados dos ativos;
c) compartilhar conta de correio eletrônico institucional;
d) acessar e divulgar informações que contenham material obsceno, apologia ao fanatismo, práticas religiosas, político partidário, qualquer forma de discriminação, bem como de material que, explícita ou implicitamente, se refira à conduta imoral;
e) fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte;
f) alimentar-se próximo aos servidores de rede e estações de trabalho;
g) fazer cópia não autorizada de softwares adquiridos ou desenvolvidos pelo Ministério Público.

Art. 6º São diretrizes relativas à operação de comunicação:
I - responsabilização pela criação, atualização, análise crítica e registro de normas, procedimentos, documentação de sistemas, recursos tecnológicos, ambiente de rede e configurações de recursos de tecnologia da informação;
II - armazenamento e disponibilização de toda e qualquer documentação institucional em local seguro, com acesso controlado e monitorado;
III - armazenamento e proteção adequada de documentos e arquivos contendo informações confidenciais;
IV - garantia da tramitação segura de documentos, no âmbito do Ministério Público;
V - manutenção sistemática da documentação institucional atualizada;
VI - exigência e obrigatoriedade da prévia análise de impacto, priorização, aprovação e plano de retrocesso para as mudanças em ativos informacionais do Ministério Público;
VII - uso de aplicações de comunicação remotas e transmissões de dados com recursos de tecnologia da informação homologados e precedidos de aprovação formal do Ministério Público;
VIII - armazenamento de informações críticas e estratégicas nos servidores da rede corporativa e em áreas protegidas;
IX - transporte de equipamentos e notebooks exclusivamente por meio de maletas apropriadas;
X - remoção de toda informação classificada como confidencial e restrita, antes de qualquer manutenção, alienação ou reutilização de equipamentos;
XI - uso único e exclusivo dos serviços de service desk do Ministério Público como suporte para solução de problemas tecnológicos ou do ambiente de tecnologia da informação;
XII - proibição de acesso à informação institucional que não seja explicitamente autorizado;
XIII - vedação do transporte de informações confidenciais do Ministério Público sem as devidas autorizações e proteções, bem como em qualquer meio, como CD, DVD, disquete, pen-drive, papel, etc.;
XIV - proibição para abrir ou executar arquivos de origem desconhecida.

Art. 7º São diretrizes relativas ao ambiente de redes:
I - normatização e regulamentação de procedimentos para a utilização correta do ambiente de rede;
II - garantia da continuidade do fornecimento de energia elétrica, em caso de interrupção, durante o tempo necessário à preservação dos equipamentos centrais de rede e dos demais que sejam essenciais;
III - garantia de estruturas de contingência para atendimento a situações emergenciais;
IV - disponibilização de recursos e estruturas tecnológicas adequadas aos padrões de segurança do Ministério Público;
V - adoção de manutenções preventivas periódicas e sistemáticas nos equipamentos instalados;
VI - liberação dos ativos de tecnologia de informação para uso, condicionada à efetiva homologação e documentação;
VII - exigência de autorização formal para a realização de intervenções e manutenções no ambiente de rede ou nas estações de trabalho;
VIII - supervisão das intervenções e manutenções realizadas no ambiente de rede;
IX - controle sistemático da utilização de equipamentos de terceiros na rede de informática do Ministério Público;
X - proteção contra ameaças externas e internas da rede e das informações que nela trafegam;
XI - monitoramento e documentação do ambiente de rede, assegurando a confidencialidade, a integridade e a disponibilidade das informações que trafegam nesse ambiente;
XII - utilização de mecanismos de segurança nas transações de rede;
XIII - manutenção de equipamentos sobressalentes de tecnologia da informação para situações emergenciais;
XIV - estruturação da rede do Ministério Público, visando à integração dos serviços de voz e dados, à facilitação do gerenciamento e ao controle da rede física, evitando eventuais violações.

Art. 8º São diretrizes relativas à internet e à intranet:
I - normatização e regulamentação de procedimentos para a utilização da internet e intranet, com a exigência de seu cumprimento;
II - adoção de ferramentas e procedimentos de segurança para os ambientes de internet e intranet;
III - restrição e controle das vulnerabilidades nos ambientes de internet e intranet;
IV - ativação e monitoramento de logs (relatórios de ocorrências) de segurança.

Art. 9º São diretrizes relativas a firewall e antivírus:
I - procedimento formal de atualização do software de firewall e antivírus em todos os ativos de informática instalados no Ministério Público, conforme instruções e determinações do fabricante;
II - manutenção sempre ativa do firewall e de programas antivírus.

Art. 10. São diretrizes relativas ao correio eletrônico:
I - normatização e regulamentação de procedimentos para o uso do correio eletrônico;
II - estabelecimento de limite máximo para o tamanho de caixa de entrada e anexos;
III - adoção de procedimentos padrões para garantir a segurança das informações veiculadas pelo correio eletrônico;
IV - garantia, junto ao provedor de serviços de e-mail, de bloqueio de relay, de modo a evitar o envio de mensagens com falsos remetentes, a partir de endereços externos ao Ministério Público;
V - utilização de sistema ou soluções de criptografia para envio e recebimento de mensagens contendo informações sigilosas ou sensíveis, por meio do correio eletrônico;
VI - encaminhamento imediato à Coordenação de Informática dos alertas de vírus recebidos pelo correio eletrônico;
VII - utilização do correio eletrônico em obediência aos padrões estabelecidos pelo Ministério Público, em portaria específica;

Art. 11. São diretrizes relativas ao desenvolvimento e à manutenção de sistemas de informação:
I - definição dos requisitos de controle de segurança para novos sistemas ou melhorias em sistemas existentes;
II - estabelecimento de mecanismos de proteção de direitos autorais para sistemas e aplicativos desenvolvidos internamente ou por terceiros;
III - definição formal das responsabilidades pelos sistemas e aplicativos, por área funcional e técnica;
IV - definição de procedimentos de validação dos dados de entrada, visando à garantia de sua correção, adequação e apropriação;
V - definição de procedimentos para validação dos dados de saída das aplicações, visando assegurar a correção, adequação e apropriação do processamento das informações armazenadas às circunstâncias;
VI - definição de procedimentos de controles criptográficos, visando à proteção das informações;
VII - impedimento do uso de bancos de dados operacionais (de produção) que contenham informações de natureza pessoal ou consideradas sensíveis, como fonte de dados de teste;
VIII - aplicação do processo de gestão de mudanças, nas alterações e mudanças nos sistemas de informações da instituição;
IX - desenvolvimento, implantação e manutenção de sistemas e aplicativos mediante adoção de metodologias e padrões de plataforma e de instalação, além de ferramentas que priorizam a segurança da informação;
X - adoção de procedimentos de contingenciamento para sistemas e aplicativos críticos, visando garantir a continuidade da ação institucional;
XI - monitoramento de todos os arquivos de logs (ocorrências) previamente configurados, visando à identificação de falhas e de violações de segurança e à recuperação de dados;
XII - manutenção de ambientes específicos, que reflitam o ambiente de produção, para desenvolvimento e homologação de sistemas;
XIII - armazenamento em ambiente seguro das versões fonte e executável de sistemas e aplicativos em desenvolvimento;
XIV - adoção de padrões de procedimentos seguros para a importação e

exportação de dados;
XV - adoção de procedimentos uniformes e padronizados para desativar sistemas e aplicativos não mais utilizados;
XVI - definição de procedimentos para supervisão e monitoramento do desenvolvimento de sistemas por empresas terceirizadas;
XVII - realização de auditorias nos sistemas de informação do Ministério Público, visando ao atendimento às conformidades legais e à minimização de riscos de interrupções nas ações institucionais.

Art. 12. São diretrizes relativas ao controle de acesso:
I - normatização e regulamentação de procedimentos de controle de acesso ao ambiente de rede, internet, intranet, serviços, aplicativos e sistemas de informações, inclusive à informação e sistemas sensíveis;
II - controle, de forma centralizada, do acesso ao ambiente e a serviços de rede, aplicativos e sistemas de informação, com a utilização de procedimentos formais, compatíveis com o perfil do usuário e com níveis de autorização;
III - controle de acesso a códigos-fonte de programa e de itens associados (projetos e especificações), prevenindo a introdução de funcionalidade não autorizada e evitando mudanças não intencionais;
IV - definição e implantação de procedimentos formais de controle para criação, alteração, bloqueio, exclusão, reutilização e expiração automática de senhas para o ambiente e serviços de rede, aplicativos, sistemas de informação, correio eletrônico, transferência de arquivos, servidores e outros;
V - implantação de padrões seguros para nomenclatura de senhas e de usuários;
VI - definição e implantação de mecanismos de gerenciamento de privilégios;
VII - controle de acesso à intranet e internet de acordo com os objetivos institucionais;
VIII - normatização e regulamentação de procedimentos e configurações seguras para os bancos de dados dos sistemas em produção, visando ao bloqueio de acessos indevidos;
IX - bloqueio ou desabilitação de usuários coletivos ou não autorizados para acessar o ambiente e serviços de rede, aplicativos, sistemas de informação, servidores e outros, e avaliação das eventuais exceções a cargo de cada unidade responsável;
X - manutenção de procedimentos para desabilitação de acessos ao ambiente e a serviços de rede, aplicativos, sistemas de informação, servidores e outros pelo tempo de sua inatividade.

Art. 13. São diretrizes relativas ao armazenamento e backup:
I - adoção de procedimentos formais de backup (cópia de segurança) e *restore* (recuperação) para todo o acervo de software e dados sob a responsabilidade do Ministério Público, de acordo com o perfil e as especificidades de utilização;
II - monitoramento e inspeção sistemática dos registros de ocorrências das rotinas de backup;
III - adoção de procedimentos para efetuar testes de recuperação, de acordo com o perfil e a especificidade da cópia de segurança;
IV - disponibilização de local adequado e seguro para o armazenamento de mídias originais de softwares e aplicativos adquiridos, juntamente com as versões definitivas e aprovadas dos sistemas de informação desenvolvidos e em produção;
V - guarda dos backups em local e ambiente adequado, seguro e distinto em relação ao local dos dados originais ou em produção.

Art. 14. São diretrizes relativas ao controle de hardware e softwares adquiridos:
I - manutenção das licenças dos softwares sempre compatíveis com o número de instalações efetuadas;
II - adoção de ferramentas e procedimentos para controle de softwares e hardwares;
III - padronização do ambiente de software;
IV - adoção de ferramentas e procedimentos para manutenções seguras, por meio de acesso remoto às estações;
V - instalação de softwares, formalmente aprovados, no ambiente de tecnologia da informação;
VI - adoção de mecanismos e medidas de controle de vazamento de informações confidenciais nos computadores portáteis em uso.

Art. 15. São diretrizes relativas à manutenção de equipamentos:
I - adoção de procedimentos para remoção de informações, consideradas relevantes, dos equipamentos liberados para manutenção, descarte, cessão de uso ou reutilização;
II - registro, controle e inspeção sistemáticos dos equipamentos de tecnologia da informação e de seus componentes;
III - estabelecimento de procedimentos para teste e homologação dos serviços de manutenção;
IV - manutenção de contrato de suporte técnico para softwares e hardwares que compõem o ambiente de tecnologia da informação;
V - adoção, nos contratos de prestação de serviços, de termo de compromisso sobre cuidados e responsabilização quanto à segurança de equipamentos de tecnologia da informação que saem para manutenção.

Art. 16. São diretrizes relativas a service desk:
I - capacitação da equipe de service desk em técnicas e práticas da engenharia social;
II - normatização e regulamentação de procedimentos para atendimento e autorização por meio do service desk;
III - instalação, nas estações de trabalho, exclusivamente de programas e softwares homologados pelo Ministério Público e realizada por profissionais e equipes de serviço indicados pelo órgão.

Art. 17. São diretrizes relativas à gestão de risco e continuidade de negócio:
I - realização sistemática de análise e avaliação dos riscos relacionados à segurança da informação do Ministério Público;
II - priorização das ações voltadas à mitigação dos riscos identificados com a implantação de novos controles que se façam necessários, como a criação de novas regras e procedimentos, a reformulação de sistemas, dentre outros;
III - estabelecimento e manutenção do plano de continuidade de negócios do Ministério Público, realizando testes e atualizações periódicas, para assegurar a sua eficácia e eficiência.

Art. 18. Compete ao Procurador-Geral de Justiça:
I - aprovar a Política de Segurança da Informação do Ministério Público do Estado do Espírito Santo;
II - baixar normas regulamentares, visando à efetiva implementação da Política de Segurança da Informação;
III - destinar recursos financeiros necessários à aquisição de hardwares e softwares apropriados para a implementação da Política de Segurança da Informação.

Art. 19. Compete à Assessoria de Planejamento e Gestão Integrada - Unidade de Tecnologia da Informação no Suporte à Gestão:
I - elaborar proposta de normas de segurança da informação na área de tecnologia da informação e as suas revisões periódicas;
II - elaborar planos de ação para implementação da Política de Segurança da Informação;
III - elaborar planos de auditoria;
IV - elaborar planos de divulgação das ações de segurança da informação implementadas;
V - acompanhar e avaliar a implementação e o desenvolvimento das ações de segurança da informação, no âmbito do Ministério Público.

Art. 20. Compete aos membros e servidores em exercício de função de chefia, coordenação ou direção, de qualquer natureza:
I - elaborar a matriz de cargos e funções da sua área, relacionando as liberações de acesso concedidas das informações sob sua responsabilidade;
II - autorizar as liberações de acesso à informação sob sua responsabilidade, de acordo com a matriz de cargos e funções, a política e as normas de segurança da informação do Ministério Público;
III - manter registro e controle atualizados das liberações de acesso à informação, reavaliando e determinando, sempre que necessário, a pronta suspensão, a alteração ou o cancelamento;
IV - identificar desvios em relação à política e às normas de segurança da informação, tomando ações corretivas necessárias.

Art. 21. Compete aos membros, servidores, estagiários e prestadores de serviço:
I - cumprir política, normas e procedimentos de segurança da informação do Ministério Público;
II - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
III - responsabilizar-se pelo cumprimento da política e das normas de segurança da informação, assinando, no caso de prestadores de serviço, o Termo de Ciência e Aceite;
IV - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Ministério Público;
V - assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades institucionais do Ministério Público;
VI - cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
VII - comunicar prontamente ao seu superior hierárquico imediato qualquer descumprimento ou violação da política, das normas e dos procedimentos de segurança da informação do Ministério Público.

Art. 22. Compete à Coordenação de Informática:
I - cumprir a política, as normas e os procedimentos de segurança da informação do Ministério Público;
II - responsabilizar-se pelo cumprimento da política e das normas de segurança da informação, assinando, no caso de prestadores de serviço, o Termo de Ciência e Aceite;
III - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Ministério Público;
IV - assegurar que os recursos tecnológicos à sua disposição sejam

utilizados apenas para as finalidades institucionais do Ministério Público;
V - operar os hardwares e softwares ligados à segurança da informação na área de tecnologia da informação;
VI - monitorar, por meio de ferramentas apropriadas, o cumprimento da política e das normas de segurança institucional, comunicando à Assessoria de Planejamento e Gestão Integrada - Unidade de Tecnologia da Informação no Suporte à Gestão, as ameaças ou violações encontradas, para providências;
VII - executar as ações de auditoria que lhe forem determinadas;
VIII - adotar as providências necessárias para aquisição de hardwares e softwares imprescindíveis para a efetivação da Política de Segurança da Informação.

Art. 23. Quaisquer violações da política e das normas de segurança da informação ensejam sanções administrativas ou legais, podendo resultar em processos administrativos, civis e criminais, caso sejam aplicáveis.

Art. 24. As aquisições de equipamentos e softwares necessários à implementação da política de segurança institucional na área de tecnologia da informação ficam sujeitas à disponibilidade orçamentária.

Art. 25. Os casos omissos serão dirimidos pelo Procurador-Geral de Justiça.

Art. 26. Ressalvado o disposto no artigo 24, esta portaria entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

Vitória, 30 de julho de 2014.
EDER PONTES DA SILVA
PROCURADOR-GERAL DE JUSTIÇA

PORTARIA Nº 4.489 de 30 de julho de 2014

O PROCURADOR-GERAL DE JUSTIÇA, no uso de suas atribuições legais, e

CONSIDERANDO o resultado e a homologação do processo de remoção por meio das Portarias nº 2.639/2014 e nº 2.971/2014;

CONSIDERANDO a Portaria nº 3.132/2014, publicada no Diário Oficial do Estado em 10 de junho de 2014, e as Portarias nº 3.910/2014 e nº 3.911/2014, publicadas em 09 de julho de 2014, que exoneraram servidores ocupantes do cargo de Agente de Apoio/Função Administrativo;

CONSIDERANDO a Portaria de nomeação nº 3.636, de 27 de junho de 2014, alterada pela Portaria nº 4.244, de 21 de julho de 2014;

FAZ SABER:

Art. 1º O resultado do **Pregão de Vagas** para o cargo efetivo de Agente de Apoio/Função: Administrativo e sua homologação:

Cargo: Agente de Apoio / Função: Administrativo			
Promotoria de Justiça	Vaga	Nome do servidor	
Promotoria de Justiça de Afonso Cláudio	1	Georgia Batista Pereira Roelke	
Promotoria de Justiça de Água Doce do Norte	1	-	
Promotoria de Justiça de Barra de São Francisco	1	-	
Promotoria de Justiça de Boa Esperança	1	-	
Promotoria de Justiça de Conceição da Barra	1	Leonardo de Aguiar Pedrini	
Promotoria de Justiça de Ibitirama	1	Cristiano Silveira Rodrigues	
Promotoria de Justiça de Iúna	1	-	
Promotoria de Justiça de Jaguaré	1	Juliana Tavares Dos Santos	
Promotoria de Justiça de Montanha	1	Stefanio Gabriel Loula Da Silva	
Promotoria de Justiça de Pedro Canário	1	-	
Promotoria de Justiça de São Gabriel da Palha	1	Jose Bemvindo Cardoso Andrade	

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Vitória, 30 de julho de 2014.
EDER PONTES DA SILVA
PROCURADOR-GERAL DE JUSTIÇA

Protocolo 77668

Protocolo MP nº 14546/2014
Primeiro Termo Aditivo ao Contrato MP nº 012/2014, celebrado entre o Ministério Público do Estado do Espírito Santo e a Arquistudio Arquitetura e Urbanismo Ltda.
- Resumo -
Objeto: objetivo prorrogar o contrato originário cujo objeto é a contratação de empresa especializada para elaboração de planilhas orçamentárias estimadas de obra civil e cronograma físico financeiro, para a futura sede da Promotoria de Justiça de Vila Velha, pelo período de 45 (quarenta e cinco) dias a contar de 30/06/2014.
Vigência: 45 dias a contar de 30/06/2014.
Gestor: Marcelo Feu Rosa Kroeff de Souza.
Ratificação: Ficam ratificadas as demais Cláusulas e condições anteriormente avençadas, não alteradas pelo presente Termo Aditivo.

Vitória, 27 de junho de 2014.
Eder Pontes da Silva
Procurador-Geral de Justiça

Contrato MP nº 039/2014
Contrato celebrado entre o Ministério Público do Estado do Espírito Santo e a Dell Computadores do Brasil Ltda.
- Resumo -
Objeto: Aquisição de 14 (catorze) computadores servidores de rede para atualização e complementação do parque tecnológico do datacenter do MP-ES, incluindo garantia dos equipamentos "*on site*".
Valor: R$ 228.200,00 (duzentos e vinte e oito mil e duzentos reais).
Vigência: 36 (trinta e seis) meses, contados a partir da data do recebimento definitivo dos equipamentos.
Gestor: Adeilson Rocha Brito.
Dotação Orçamentária: Este contrato correrá através da Atividade nº 03.126.0296.4050 - Gestão de tecnologia da informação, Elemento de Despesa 4.4.90.52.35 - Equipamentos e material permanente - Equipamentos de processamentos de dados.

Vitória, 30 de julho de 2014.
Eder Pontes da Silva
Procurador-Geral de Justiça
Protocolo 77653

Primeiro Termo Aditivo ao Convênio MP nº 006/2014, celebrado entre o Ministério Público do Estado do Espírito Santo e a Sociedade de Ensino Superior de Vitória Ltda.
- Resumo -
Objeto: Alterar a Cláusula Primeira, do Convênio MPES Nº 006/2014, para incluir no seu objeto o oferecimento de vagas de estágio supervisionado a estudantes da **FACULDADE DE DIREITO DE VITÓRIA - FDV** de cursos de pós-graduação conforme Portaria nº 4.247 de 21 de julho de 2014, publicada no Diário Oficial do Estado do Espírito Santo no dia 22 de julho de 2014, na forma da Lei Federal nº 9.394/1996 e conforme autorização do Procurador-Geral de Justiça no bojo do processo administrativo nº 10.231/2014.
Vigência: a contar do dia subsequente à publicação do seu extrato no Diário Oficial do Estado do Espírito Santo.
Ratificação: Ficam ratificadas as demais Cláusulas e condições anteriormente avençadas, não alteradas pelo presente Termo Aditivo.

Vitória, 29 de julho de 2014.
Eder Pontes da Silva
Procurador-Geral de Justiça
Protocolo 77654

Errata de Extrato do Segundo Termo Aditivo ao Contrato MP nº 048/2012.
Processo MP nº 12997/2012.

Na publicação do Segundo Termo Aditivo ao Contrato MP nº 048/2012, publicado no Diário Oficial do dia 29/07/2014.

Onde se lê:
Gestor: Adeilson Rocha Brito.

Leia-se:
Gestor: Jafeth Rodor Ramos.

Vitória, 29 de julho de 2014.
Eder Pontes da Silva
Procurador-Geral de Justiça

Errata de Extrato do Terceiro Termo Aditivo ao Contrato MP nº 079/2013.
Processo MP nº 2683/2014.

Na publicação do Terceiro Termo Aditivo ao Contrato MP nº 079/2013, publicado no Diário Oficial do dia 16/07/2014.

Onde se lê:
Vigênica: 90 dias, a contar de 04/04/2014.

Leia-se:
Vigência: 180 dias, a contar de 04/04/2014.

Vitória, 30 de julho de 2014.
Eder Pontes da Silva
Procurador-Geral de Justiça
Protocolo 77656

Gerência Geral

PORTARIAS DA SENHORA GERENTE-GERAL:
A GERENTE-GERAL, no uso de suas atribuições legais, assinou as seguintes Portarias:

PORTARIA Nº 4.490 de 30 de Julho de 2014
CONCEDER licença para tratamento de saúde, por 02 dias, a servidora AMANDA CUNHA HEIZER ABDALA, a partir de 24/07/2014, na forma do art. 129, da Lei Complementar nº 46/94 de 31/01/94, conforme Procedimento MP/Nº 32483/2014.

PORTARIA Nº 4.491 de 30 de Julho de 2014
CONCEDER licença para tratamento de saúde a servidora