DIÁRIO OFICIAL ELETRÔNICO
DEFENSORIA PÚBLICA DO ESTADO DA BAHIA

Salvador, Bahia
Quarta-feira
09 de Novembro de 2022
Ano I • nº 850

SUMÁRIO

Defensoria Pública do Estado da Bahia
Avenida Ulisses Guimarães, nº 3.386, Edf. MultiCab Empresarial
CEP - 41.219-400, Sussuarana, Salvador/Bahia
Ouvidoria 3117-6936 | 6952

GABINETE DO DEFENSOR PÚBLICO GERAL

PORTARIA Nº 1345/2022, DE 08 DE NOVEMBRO DE 2022.

Institui a Política de Segurança da Informação - PSI.

O DEFENSOR PÚBLICO GERAL DO ESTADO DA BAHIA, no uso de suas atribuições, conferidas pelo art. 32 da Lei Complementar Estadual nº 26/2006, com as alterações da Lei Complementar Estadual nº 46/2018, RESOLVE publicar a presente PSI - Política de Segurança da Informação no âmbito da Defensoria Pública do Estado da Bahia.

Gabinete do Defensor Público Geral, em 08 de novembro de 2022.

RAFSON SARAIVA XIMENES
Defensor Público Geral

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

O cenário tecnológico mundial tem evoluído rapidamente, proporcionando cada vez mais facilidades, tanto no uso e armazenamento das informações, quanto na sua transmissão por redes de computadores privadas ou pela Internet. Essa evolução, no entanto, traz consigo um aumento considerável dos riscos aos ambientes tecnológicos das organizações e, consequentemente, às informações sob sua responsabilidade. Com isso, medidas devem ser aplicadas para prover garantias a essas informações, buscando resguardar aqueles que são considerados os principais pilares da Segurança da Informação:

Confidencialidade: toda informação, esteja ela em meio eletrônico ou não, deve estar acessível somente a quem tem o direito a este acesso. Mecanismos de processos e tecnologias devem ser implementados buscando satisfazer esta premissa.

Integridade: toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada.

Disponibilidade: as informações devem estar sempre disponíveis para os usuários que dela necessitarem e que tenham autorização para tal acesso.

Autenticidade: devem ser adotados mecanismos que garantam a autenticidade e rastreabilidade dos(as) usuários(as) na utilização dos recursos computacionais, de forma a tornar possível a identificação dos(as) autores(as) de qualquer ação que seja feita utilizando os sistemas informatizados e meios de comunicação.

Irretratabilidade: esse pilar parte do princípio jurídico da irretratabilidade, no qual não se pode negar a origem da informação fornecida. Aplica-se principalmente em casos de certificados on- line, transações e assinaturas digitais.

APLICAÇÕES

As diretrizes aqui estabelecidas deverão ser seguidas por todos(as) os(as) defensores(as), servidores(as), estagiários(as), bem como os(as) prestadores(as) de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador(a) de que os ambientes, sistemas, computadores e redes da DPE/BA poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador(a) se manter atualizado(a) em relação a este regulamento e aos procedimentos e normas relacionadas, bem como aplicá-la, buscando orientação do(a) seu(sua) gestor(a) ou da Coordenação de Modernização e Informática sempre que não estiver absolutamente seguro(a) quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS

Toda informação produzida ou recebida pelos(as) colaboradores(as) como resultado da atividade profissional contratada pela Defensoria Pública do Estado da Bahia pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os recursos de informática disponibilizados pela DPE/BA são fornecidos com o propósito único de garantir o desempenho das atividades de cada membro, servidor(a) ou eventual colaborador(a), sendo vedado o uso desses recursos para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, veicular opiniões político-partidárias, religiosas e quaisquer outras atividades que contrariem os objetivos institucionais.

A Defensoria Pública, por meio da Coordenação de Modernização e Informática, poderá registrar todo o uso dos sistemas e serviços, visando garantir a segurança das informações utilizadas.

REQUISITOS

Para a uniformidade da informação, a PSI deverá ser comunicada a todos(as) os(as) colaboradores(as) da Defensoria Pública do Estado da Bahia, para que as normas estabelecidas sejam cumpridas dentro e fora da instituição.

Este documento deverá ser revisto e atualizado periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Administração Superior.

Deverá constar em todos os contratos que envolvem a Coordenação de Modernização e Informática o termo de responsabilidade e sigilo, como condição

imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.
A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos(as) colaboradores(as).
Todos(as) os(as) colaboradores(as) devem ser orientados(as) sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.
Todo incidente que afete a segurança da informação deverá ser comunicado à Central de Atendimento ao Usuário e aos Encarregados de Proteção de Dados o mais breve possível e quando necessário a CMO fará as diligências necessárias.
Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de transição.
Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.
Estas diretrizes deverão ser implementadas na Defensoria Pública do Estado da Bahia por meio de procedimentos específicos, obrigatórios para todos(as) os(as) colaboradores(as), independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviço.
O não cumprimento dos requisitos previstos nas Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o(a) usuário(a) às medidas administrativas e legais cabíveis.

PAPÉIS E RESPONSABILIDADES
É papel:
De todos os membros, servidores(as) e demais colaboradores(as) da DPE/BA: conhecer e seguir as regras definidas nesta Política de Segurança da Informação, sob pena de responsabilização em caso de seu descumprimento e possível sanção disciplinar.
De todo(a) gestor(a): ter postura exemplar em relação à Segurança da Informação e disseminar as boas práticas definidas pela DPE/BA em sua área de atuação, sendo de sua responsabilidade gerir os acessos dos membros, servidores(as) e demais colaboradores(as) da DPE/BA nos sistemas de informação da instituição, a fim de minimizar riscos de que acessos indevidos ocasionem vazamentos de informação.
Do Comitê de Segurança da Informação: contribuir para a constante evolução da Segurança da Informação na instituição, reunindo-se periodicamente para analisar temas relevantes sobre Segurança da Informação e sua aplicabilidade na DPE/BA.
Também é papel do Comitê definir e gerir processos de Segurança da Informação, propor projetos em Segurança da Informação, propor alterações e aprovar a Política de Segurança da Informação, bem como seus documentos complementares.
Da Coordenação de Modernização e Informática: realizar o apoio técnico e operacional no planejamento estratégico da segurança institucional de TI para a implantação e manutenção das tecnologias empregadas na Política de Segurança da Informação e propor investimentos e projetos em Segurança da Informação, além de garantir que os sistemas e ambiente tecnológico utilizados pelos membros, servidores(as), demais colaboradores(as) e usuários(as) dos sistemas e equipamentos da DPE/BA forneçam proteção adequada às informações durante todo o seu ciclo de vida (criação, armazenamento, uso, transferência, arquivamento e descarte).
Dos(as) gestores(as) e fiscais dos contratos de prestação de serviço: o registro e manutenção, no sistema de controle de acesso, dos dados dos(as) funcionários(as) vinculados(as) aos respectivos contratos.

CUSTODIANTES DA INFORMAÇÃO
CABE À COORDENAÇÃO DE MODERNIZAÇÃO E INFORMÁTICA:
Testar a eficácia dos controles utilizados e informar aos(às) gestores(as) os riscos residuais. Configurar os equipamentos, ferramentas e sistemas concedidos aos(às) colaboradores(as) com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por este regulamento, e pelas Normas de Segurança da Informação complementares.
Os(as) administradores(as) e operadores(as) dos sistemas computacionais podem, pela característica de seus privilégios como usuários(as), acessar os arquivos e dados de outros(as) usuários(as). No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
Garantir segurança especial para sistemas com acesso público, incluindo o ambiente institucional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Defensoria Pública.
O(a) gestor(a) da informação deve ser previamente informado(a) sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo(a) custodiante.
Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um(a) responsável identificável como pessoa física, sendo que:
a) Os usuários (logins) individuais de funcionários(as) são de responsabilidade do(a) próprio(a) funcionário(a).
b) Os usuários (logins) de terceiros serão de responsabilidade do(a) gestor(a) da área contratante.
Proteger continuamente todos os ativos de informação da DPE-BA contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente institucional, exigindo o seu cumprimento dentro da Defensoria Pública.
Realizar auditorias periódicas de configurações técnicas e análise de riscos.
Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários(as) por motivo de desligamento da Defensoria Pública do Estado da Bahia, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Defensoria Pública do Estado da Bahia.
Monitorar o ambiente de TI, gerando indicadores e históricos de:
a) Uso da capacidade instalada da rede e dos equipamentos;
b) Tempo de resposta no acesso à internet e aos sistemas críticos da DPE-BA;
c) Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da DPE-BA;
d) Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
e) Atividade de todos(as) os(as) colaboradores(as) durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).
Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
Propor e apoiar iniciativas que visem à segurança dos ativos de informação da DPE-BA.
Publicar e promover as versões da Política de Segurança da Informação e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação do Estado da Bahia.
Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação e Administração Superior da DPE-BA.
Buscar alinhamento com as diretrizes corporativas da instituição.

CABE À COORDENAÇÃO DE RECURSOS HUMANOS:
Solicitar à CMO ajuste de perfil de acesso, quando houver transferência de setor.
Solicitar imediatamente a CMO eliminação do login, quando houver saída de pessoal, tanto do quadro permanente, quanto do quadro temporário.

CABE AO COMITÊ DE SEGURANÇA DA INFORMAÇÃO
Reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a Defensoria Pública.
O Comitê poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
Avaliar os incidentes de segurança e propor ações corretivas;
Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação.

CAPACITAÇÃO E CONSCIENTIZAÇÃO
É de responsabilidade do Comitê de Segurança da Informação prover treinamento sobre Segurança da Informação a todos os membros, servidores(as) e demais colaboradores(as), bem como realizar atividades pontuais para aumentar a conscientização com relação a este assunto.
Essas atividades podem ser realizadas através de cursos on-line EAD, mensagens eletrônicas disparadas periodicamente, notícias e dicas de utilização disponibilizadas no e-mail coorporativo, eventos anuais de Segurança da Informação, entre outras atividades.

REVISÃO:
Esta Política de Segurança da Informação e seus documentos complementares devem ser revisados criticamente ao menos uma (01) vez ao ano, ou toda vez que houver uma alteração significativa no ambiente computacional ou organizacional.
A responsabilidade por iniciar a revisão é da CMO e do Comitê Gestor de Segurança da Informação, que deve revisar e aprovar as modificações realizadas na documentação.

PROPRIEDADE INTELECTUAL
Todo o conteúdo desenvolvido pelos membros, servidores(as) e demais

colaboradores(as) da DPE/BA durante o horário do expediente, nas dependências da DPE/BA ou remotamente, com a finalidade de atender especificamente as atividades da DPE/BA é de propriedade da DPE/BA.
Estão incluídos nesses itens planilhas, fórmulas, formulários, fluxos de trabalho, código fonte de sistemas e aplicações, scripts de automação, etc.

UTILIZAÇÃO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO
Todo o gerenciamento dos equipamentos e dos Sistemas de Informação da Defensoria Pública do Estado da Bahia é de responsabilidade da Coordenação de Modernização e Informática.
A responsabilidade pela conservação de cada equipamento é do membro, servidor(a) e/ou eventual colaborador(a) que o utiliza diariamente.
O transporte dos equipamentos deve ser realizado em mochila ou mala apropriada, para evitar danos ao mesmo. Durante seu trânsito, o membro, servidor(a) ou eventual colaborador(a) deverá ter o equipamento sempre consigo, não o deixando desacompanhado, seja no carro, em ambientes externos, aeroportos, hotel, etc.
Nenhum equipamento deve ser deixado ligado ou desprotegido de senha no descanso de tela quando não estiverem em uso.
É de responsabilidade dos membros, servidores(as), demais colaboradores(as) e prestadores(as) de serviços que os utilizam assegurarem o cumprimento desse requisito.
Ao se ausentar da mesa, mesmo que por um curto período, o computador deverá ser bloqueado usando as teclas CTRL + ALT + DEL e bloquear estação.
Não é permitido instalar softwares sem o conhecimento da CMO. Toda necessidade de instalação de novo programa ou software deve ser formalizada via abertura de chamado por meio do servicedesk, para que possa ser devidamente analisada pela área, observando as regras internas e sem prejudicar a segurança da instituição como um todo.
A manutenção física dos equipamentos (adição, remoção e substituição de hardware) é de responsabilidade da CMO, sendo proibido aos membros, servidores(as) e demais colaboradores(as) da DPE/BA de outras áreas a execução dessas atividades.
Os equipamentos disponibilizados pela DPE/BA a seus membros, servidores(as) e demais colaboradores(as) são para uso profissional, relacionado às atividades da instituição.
É vedada a utilização de equipamentos pertencente a DPE/BA para meios ilícitos, como por exemplo envio de material sexualmente explícito ou implícito; conteúdo ofensivo, preconceituoso ou discriminatório; apologia à violência ou atos terroristas; apologia às drogas; violação de direitos autorais; acessos não autorizados a equipamentos de terceiros; qualquer tipo de atividade relacionada a fraude; entre outros.
O membro, servidor(a) e demais colaboradores(as) da DPE/BA devem prezar pela individualidade de suas credenciais de acesso, não podendo, em hipótese alguma, compartilhar seu login e senha de acesso aos sistemas e sites corporativos. Também é sua responsabilidade garantir que senhas seguras sejam utilizadas.

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS
Em todas as estações de trabalho e servidores deverão ter instaladas ferramentas de proteção contra códigos maliciosos, como vírus, worms, ramsonwares e etc. A definição da ferramenta a ser utilizada e as regras de configuração e atualização são de responsabilidade da CMO, bem como a responsabilidade por instalar e manter a ferramenta antivírus operacional nos servidores e estações de trabalho.
Fora do ambiente computacional da DPE/BA, o próprio membro, servidor(a) ou eventual colaborador(a) é o(a) responsável pela atualização do software de antivírus e execução de varredura em equipamento pertencente a DPE/BA sob sua responsabilidade.

DIVULGAÇÃO DE INFORMAÇÕES
Todas as informações da DPE/BA independente do formato em que se encontram (gravadas em meios magnéticos, impressas, entre outros), devem ser protegidas pelo(a) proprietário(a) da informação, de maneira proporcional ao seu grau de importância e classificação.
Toda e qualquer informação relacionada às atividades da DPE/BA, gerada, adquirida, utilizada ou armazenada nos ativos de informação da DPE/BA, seja por seus membros, servidores(as), colaboradores(as) ou terceiros, é considerada seu patrimônio e deve ser protegida conforme estabelecido na legislação vigente.
Na necessidade do envio de informações confidenciais para pessoas externas à organização, o envio deve ser realizado utilizando os canais oficiais da instituição, como o e-mail corporativo e soluções internas de compartilhamento e arquivos.
Documentos impressos devem ser recolhidos logo após sua geração ou emissão, não podendo ser mantidos nos aparelhos ou sobre as mesas, ao alcance de todos.
Arquivos, documentos e mensagens eletrônicas que não mais necessários e/ou obsoletos deverão ser inutilizados e descartados.

CONTRATOS E ACORDOS COMERCIAIS
Nenhuma atividade que envolva a contratação de prestadores(as) de serviço (envolvendo cessão de mão-de-obra ou não) deverá ser iniciada sem a devida formalização do respectivo contrato, o que pressupõe planejamento por parte da área contratante quanto à inserção da Consultoria Jurídica no negócio a ser firmado, de modo a permitir a elaboração dos trabalhos em tempo hábil.
Os contratos de serviços de terceiros devem ser validados sob os aspectos técnico, operacional e comercial, pelos(as) responsáveis(as) pela contratação, de acordo com os padrões da DPE/BA.
Todos os contratos com os(as) prestadores(as) de serviço devem conter cláusula específica de sigilo e confidencialidade em relação a toda e qualquer informação da DPE/BA a que este(a) prestador(a) tenha acesso.
Quando o contrato abranger atividades correlatas a Engenharia de Software, como desenvolvimento, melhoria ou manutenção de sistemas de informação, cujo produto se destine ao uso pela DPE/BA, todos os artefatos produzidos, inclusive código-fonte, no escopo deste contrato, pertencerão a DPE/BA, não sendo possível sua divulgação ou reutilização externa, salvo autorização expressa da DPE/BA.

DISPOSITIVOS DE ARMAZENAMENTO EXTERNO
Os(as) usuários(as) de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos que podem danificar e corromper dados, assim como viabilizar o vazamento de informações corporativas confidenciais.
Seu uso exige cautela, para reduzir o risco tanto de vazamento de informações internas, quanto o comprometimento do equipamento/rede através de softwares maliciosos.
Ao encontrar algum pendrive ou mídia removível perdido pelas dependências da DPE/BA, a instrução é para que o mesmo seja levado até a CMO para análise prévia.

ACESSO REMOTO
O padrão para permitir que membros, servidores(as) e demais colaboradores(as) da DPE/BA se conectem remotamente nas redes da DPE/BA é a VPN (Virtual Private Network). Nenhuma outra forma de acesso remoto é permitida.
A utilização desse recurso requer um acesso à Internet, fazendo com que sua conexão à internet seja estabelecida antes de se conectar à VPN da DPE/BA. Como o(a) usuário(a) pode utilizar esse recurso através de hotéis, residências e afins, os problemas de acesso à Internet nesses lugares devem ser sanados antes de se iniciar a conexão remota com a DPE/BA. Uma vez conectado à VPN, o(a) usuário(a) deverá acessar apenas o recurso de destino para o qual o acesso foi designado.
Os métodos de conexão à VPN e os grupos de membros, servidores(as) e demais colaboradores(as) da DPE/BA a quem se destina cada método são definidos pela CMO, e podem variar de acordo com a tecnologia utilizada.
O(a) colaborador(a) que dispõe de acesso à VPN não pode, em hipótese alguma, compartilhar seu usuário(login) e senha com outras pessoas.
A DPE/BA possui a autonomia de bloquear o acesso de um(a) determinado(a) usuário(a), ou mesmo desabilitar o serviço de VPN, a qualquer momento, caso seja detectada uma ameaça de segurança ou qualquer outra anormalidade nesse serviço que implique em risco à segurança da informação.

ACESSO REMOTO PARA FUNCIONÁRIOS(AS)
O membro, servidor(a) ou eventual colaborador(a) pode requerer acesso remoto à VPN da DPE/BA uma vez que identifique a necessidade de atuar com ferramentas, ou acessar informações presentes apenas internamente na instituição, enquanto ele se encontra fisicamente fora das dependências da instituição.
Este acesso requer a aprovação formal de(a) seu(a) superior, e as regras para este tipo de atuação seguem as mesmas regras de quando o(a) servidor(a) ou colaborador(a) está atuando localmente em seu ambiente de trabalho usual (dentro das dependências da instituição).
Desde que se comprove a real necessidade, e que haja possibilidade da CMO, é recomendado testar a configuração previamente, junto com o(a) usuário(a) que irá utilizar o acesso remoto.

CONTROLE REMOTO PARA SUPORTE
O acesso aos computadores através da ferramenta de controle remoto deve ser utilizado apenas para suporte das equipes de atendimento ao(à) usuário(a) da CMO.
O(a) usuário(a) deverá informar o nº ID do equipamento e aprovar o acesso.

USO DE CREDENCIAIS DE ACESSO
Os dispositivos de identificação e senhas protegem a identidade do(a) colaborador(a) usuário(a), evitando e prevenindo que uma pessoa se faça passar por outra perante a Defensoria Pública e/ou terceiros.
O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
A utilização indevida das informações obtidas em razão de acesso aos sistemas, atendimentos entre outras formas de coleta de informações, poderá se enquadrar nos tipos penais previstos nos artigos 319 (prevaricação), 320 (condescendência criminosa), 321 (advocacia administrativa), 325 (violação do sigilo funcional) e 326 (violação do sigilo de proposta de concorrência pública) do Código Penal.
A autenticação é a forma mais básica para controlar acesso a sistemas computacionais. Ela nos permite controlar entre outras coisas:
a) Quem terá acesso a um sistema;
b) Qual será o nível de acesso;
c) Qual será o período de vigência do acesso.
Diante do grau de importância deste mecanismo, para que consigamos um nível

adequado de controle, devemos prezar pela guarda desta credencial.
Algumas recomendações referentes à composição e uso de senhas de acesso, com o objetivo de assegurar sua confidencialidade:
Recomenda-se que a senha seja trocada imediatamente após o primeiro acesso. Depois disso, a troca deve ser efetuada mediante solicitação automática do sistema;
Recomenda-se que seja composta por, pelo menos, oito (08) caracteres. É importante ressaltar que, quanto maior a senha, maior a dificuldade em decifrá-la;
Uma boa senha deve ser composta de letras maiúsculas e minúsculas, ditos numéricos e caracteres especiais (ex: #, @,$, %, &), além de não ser uma palavra que possa ser encontrada em dicionários em qualquer língua;
Não devem ser utilizadas senhas com nomes próprios, números de telefone, nome da conta no sistema, datas de aniversário, caracteres idênticos repetidos (ex:11111, aaaaa) ou sequenciais (ex: abcdef, 12345);
Evite reutilizar senhas antigas;
Não se deve guardar anotações de senhas em blocos de anotações, post-it nos monitores, embaixo dos teclados, anotado no calendário, embaixo do aparelho telefônico, agendas ou qualquer local de fácil acesso;
Cada usuário(a) é inteiramente responsável pelo uso de sua conta de acesso à rede, suas senhas e outros tipos de autorização, que são de uso individual e intransferível, e não podem ser compartilhados com colegas de trabalho ou terceiros. Nessa situação, o membro, servidor(a) ou eventual colaborador(a) será responsável por ações indevidas que venham a ser efetuadas a partir de sua conta de acesso à rede ou sistemas, caso alguém obtenha acesso à sua conta devido a não utilização de senhas seguras;
A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas.
Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.
Portanto, assim que algum(a) usuário(a) for demitido(a) ou solicitar demissão a Coordenação de Administração de Pessoal deverá imediatamente comunicar tal fato a CMO, a fim de que essa providência seja tomada.
A Coordenação de Compras e Serviços Administrativos deverá comunicar imediatamente à CMO o desligamento dos(as) colaboradores(as) terceirizados(as).
A mesma conduta se aplica aos (às) usuários(as) cujo contrato ou prestação de serviços tenha se encerrado, bem como aos(às) usuários(as) de testes e outras situações similares.

ENVIO DE SENHAS
Após a criação de uma nova conta, as credenciais serão enviadas para os(as) usuários(as), seguindo as regras abaixo:
A senha de acesso à rede ou webmail, deverá ser enviada para o e-mail corporativo do(a) superior imediato(a), ou seu(sua) representante devidamente autorizado.
Para os demais sistemas, a senha deverá ser enviada diretamente para o respectivo e-mail corporativo. Para funcionários(as) terceirizados(as), a senha deverá ser enviada para o e-mail corporativo do(a) superior imediato(a), ou seu(sua) representante devidamente autorizado(a).

USO DO CORREIO ELETRÔNICO
O e-mail funcional é um meio de comunicação de uso exclusivo para trabalhos da instituição. A liberação cabe à coordenação da área, que deverá avaliar a necessidade e solicitar a CMO.
A conta de correio funcional (e-mail) é individual, não podendo ser compartilhada com outros membros, servidores(as) e/ou colaboradores(as) da CMO. Os eventuais casos especiais deverão ser devidamente analisados.
É vedada a utilização do e-mail corporativo para cadastro em sites de redes sociais, relacionamento e de empresas.
Nos casos das contas departamentais, um(a) usuário(a) deverá ser o(a) responsável formal por realizar as manutenções nessa caixa de entrada, gerenciando o espaço disponível. Esse(a) usuário(a) também é responsável pelo conteúdo das mensagens recebidas e enviadas.

DAS RESTRIÇÕES NO USO DO CORREIO ELETRÔNICO INSTITUCIONAL
Assuntos particulares não devem ser enviados pelo e-mail institucional.
O envio de mensagens com destino a todos(as) os(as) usuários(as) somente deve ser utilizado se o assunto for relacionado diretamente aos negócios da instituição e se realmente todos devem receber aquela mensagem;
Não enviar, armazenar ou manusear material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Política de Segurança da Informação e suas normas, lesivos aos direitos e interesses da DPE/BA ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
Não enviar, armazenar ou manusear material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais, e o uso extensivo para assuntos particulares.
A utilização de webmails particulares por parte dos membros, servidores(as) e demais colaboradores(as) da DPE/BA não é proibida, porém todo e qualquer assunto relacionado às atividades exercidas na DPE/BA deve ser tratado exclusivamente pelo endereço de e-mail corporativo.

USO DA INTERNET
Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os(as) usuários(as) devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e utilizar seus recursos;
O acesso à Internet via rede da DPE/BA, seja por conexão a cabo, modem ou wifi, é um meio de comunicação para atividades da instituição.
A responsabilidade de liberação destes acessos cabe ao(à) responsável da área requisitante, que deverá avaliar a necessidade e solicitar a CMO através de chamado.
Qualquer membro, servidor(a), ou eventual colaborador(a) que tenha acesso a um computador e à rede da DPE/BA poderá utilizar a Internet, desde que tenha a devida aprovação do(a) seu(a) superior.
Os níveis de acesso são definidos pela CMO, e as categorias de sites permitidos e bloqueados em cada categoria também.
A citação de categorias de determinados sites proibidos, descritos no decorrer deste documento serve apenas para exemplificar e facilitar o entendimento, fazendo com que essa lista não seja restrita a somente este tipo de conteúdo.
A utilização da rede de INTERNET da Defensoria Pública do Estado da Bahia deve obedecer aos seguintes critérios:
Todo acesso à Internet da DPE/BA deve ser feito utilizando equipamentos e métodos de acesso providos e autorizados pela DPE/BA;
Os membros, servidores(as) e demais colaboradores(as) da DPE/BA devem abster-se de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da DPE/BA, de terceiros ou que de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software) da instituição ou de terceiros, bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;
O acesso a qualquer conteúdo que esteja em desacordo com essa prática, como sites de conteúdo sexual, pedofilia, discriminação de qualquer tipo, jogos, salas de bate-papo, web messengers, comunidades virtuais, serviços de proxy público, incentivo a atos ilícitos e afins, dentro do ambiente de trabalho, ainda que fora do horário do expediente, é terminantemente proibido;
A CMO pode determinar quais os tipos de arquivo que podem ser copiados da internet para a rede interna, através de download;
O acesso a webmails particulares, como UOL, TERRA, GMAIL, YAHOO, HOTMAIL etc. é limitado ao uso pessoal, não podendo ser utilizado para troca de informações da DPE/BA;
Devido ao bloqueio de sites ser baseado em um sistema automatizado, algumas páginas poderão ser bloqueadas inadvertidamente. Caso seja bloqueado um site cujo conteúdo seja de utilidade para o trabalho, o(a) usuário(a) pode solicitar o desbloqueio à CMO, através de chamado no servicedesk.
O fato de um site não estar bloqueado não significa que o mesmo possa ser acessado pelos usuários. Deverão ser observados todos os preceitos desta Norma.

UTILIZAÇÃO DO SERVIDOR DE ARQUIVOS
Todos os arquivos ou documentos institucionais da DPE/BA deverão estar armazenados em um diretório (pasta), disponibilizada pela CMO no servidor de arquivos, onde este estiver disponível.
A criação e/ou manutenção desta pasta será efetuada mediante solicitação a CMO através de chamado no servicedesk.
Todos os documentos armazenados no servidor de arquivos possuem cópia de segurança (backup).
A CMO não se responsabilizará pelo backup dos dados gravados pelos(as) usuários(as) fora das áreas especificamente disponibilizadas para o seu setor no servidor de arquivos, devendo, os(as) usuários(as) manter backup regulares destes dados.
Os critérios, procedimentos e periodicidade para realização das cópias de segurança, bem como o tempo de retenção de arquivo(s) e/ou pastas são estabelecidos pela CMO. As solicitações de restauração de arquivos devem ser realizadas através da ferramenta de chamados e a CMO possui 48 horas para disponibilizar os arquivos restaurados.
A análise dos tipos de arquivos permitidos no servidor de arquivos é de responsabilidade da CMO, podendo ser alterada a qualquer momento. O armazenamento de arquivos poderá conter todo tipo de arquivo (*.docx., *.xlsx, *.pptx, *.jpg.), exceto arquivos executáveis ou que não tenham ligação direta com as funções do proprietário do mesmo (*.avi, *.rm, *.mp3,*.mp4, *.mdb, *.mdf.). Casos especiais deverão ser analisados pela CMO.
A manutenção do espaço destinado a cada área é de responsabilidade da própria área, que deve gerenciar os arquivos existentes e realizar a remoção e compactação de arquivos antigos ou que não são mais utilizados.
Caso após a remoção e compactação de arquivos, o espaço for insuficiente, a CMO deve ser contatada para avaliar as necessidades e possibilidades de aumento do espaço.

USO DE EQUIPAMENTOS PORTÁTEIS
Não são permitidas alterações de configurações no hardware, no sistema operacional e de padrões dos aplicativos disponibilizados nos equipamentos cedidos pela Defensoria Pública para trabalho externo, estando o membro, servidor(a) ou eventual colaborador(a) infrator(a) sujeito(a) às sanções disciplinares da Política de Segurança da Informação, bem como, responsabilizado(a) pelos danos causados aos referidos equipamentos.
O equipamento cedido ao servidor(a) ou eventual colaborador(a) deve ser utilizado para a execução das atividades relacionadas a DPE/BA.
As informações armazenadas nos equipamentos cedidos pela instituição não devem, em hipótese alguma, ser distribuídas, copiadas, compartilhadas ou cedidas para quem quer que seja, em qualquer meio, seja impresso, magnético ou transcrito sem justificativa válida de interesse da Instituição.
É de responsabilidade do membro, servidor(a) ou colaborador(a) a salvaguarda das informações armazenadas nos equipamentos portáteis, uma vez que o disco rígido do equipamento é passível a falhas.
Em caso de falha em qualquer dispositivo do equipamento em questão, o(a) usuário(a) não deverá procurar assistência técnica ou fazer qualquer substituição de componentes (disco rígido, baterias, carregadores, antenas etc.) sem a autorização prévia da CMO.
Em caso de roubo, furto, perda total ou parcial do equipamento recebido, o(a) usuário(a) deverá comunicar imediatamente seu superior, bem como à CMO, e providenciar o registro do respectivo boletim de ocorrência (BO) junto à autoridade policial.
Todas as regras citadas acima valem para notebooks, celulares, smartphones, etc., fornecidos pela DPE/BA a seus membros, servidores(as) e eventuais colaboradores(as).
Quando em viagem, e sempre que possível, os computadores portáteis devem ser levados como bagagem de mão, tendo em vista critérios de segurança da informação.

USO DE EQUIPAMENTOS PORTÁTEIS PARTICULARES
Funcionários(as) que preferirem utilizar seus equipamentos particulares para fins institucionais só poderão fazê-lo com autorização explícita da CMO. O uso só poderá ocorrer após análise do equipamento pela equipe técnica responsável, para garantir que ferramentas mínimas de proteção estejam instaladas no equipamento em questão, bem como padrões minimamente aceitáveis de hardware e software definidos pela CMO.
Se após a análise, o equipamento não estiver dentro dos padrões aceitáveis, a CMO poderá sugerir a utilização de um equipamento institucional, se houver disponibilidade, ou a adequação do equipamento do membro, servidor(a) ou eventual colaborador(a) para que sua utilização seja permitida.
Requisitos mínimos aceitáveis incluem:
I . Versão de sistema operacional suportado pelo fabricante e com as últimas atualizações devidamente instaladas;
II. Software antivírus instalado e atualizado;
III. Programas devidamente licenciados (poderá ser solicitada a exibição da licença ou nota fiscal dos aplicativos para comprovação);
IV. Utilização de usuário(login) e senha para autenticação no sistema operacional;
V. Utilização de programa para criptografia de disco (opcional).
Se for decidido por adequar o equipamento às regras da DPE/BA, somente após as devidas correções serem realizadas é que seu uso será permitido.
Em equipamentos particulares, os dados pessoais deverão ficar armazenados em diretório distinto das informações institucionais.

AUDITORIA
Os acessos realizados por membros, servidores(as) ou eventuais colaboradores(as), utilizando-se da rede da Defensoria Pública, mesmo os realizados através dos equipamentos particulares, poderão ser auditados em casos de eventos que comprometam a segurança das informações.
Os equipamentos de propriedade da DPE/BA poderão ser auditados em casos de eventos que comprometam a segurança das informações.

GESTÃO DE ATIVOS
Todas as regras para instalação de hardware e software, manutenção e movimentação de equipamentos de informática estão definidas na portaria Nº 986/2021, DE 25 DE OUTUBRO DE 2021 que regulamenta o uso dos recursos de tecnologia da informação no âmbito da Defensoria Pública do Estado da Bahia.

AQUISIÇÃO DE BENS DE TI
As áreas do DPE não podem efetuar aquisições de recursos de informática interagindo diretamente com os(as) fornecedores(as).
Para aquisição de SOFTWARES, a CMO deverá ser antes contatada para as devidas providências.

ARMAZENAMENTO DE MÍDIAS E LICENÇAS
Todas as mídias de instalação de software (CD-ROM, DVD, etc.) e as respectivas licenças de uso devem ser catalogadas e armazenadas pela CMO. Os manuais operacionais devem permanecer no setor sob a responsabilidade do(a) usuário(a).

INSTALAÇÃO DE SOFTWARES
Somente a CMO está autorizada a efetuar instalações de softwares nas estações de trabalho e servidores.

GERENCIAMENTO DE ACESSOS
Os sistemas de informação são ativos importantes para a instituição. Todos os membros, servidores(as) e demais colaboradores(as) tem a responsabilidade de manter os recursos de tecnologia da informação protegidos contra ameaças, tais como: acesso indevido e não autorizado, divulgação não autorizada, erros, etc.
A gestão das práticas de segurança da informação é de responsabilidade do Comitê de Segurança da informação, com apoio técnico da Coordenação de Modernização e Informática (CMO), que direcionará todas as questões relacionadas a este tópico.
A mesma é também responsável por elaborar, revisar, submeter à aprovação e atualizar periodicamente esta norma, bem como em criar procedimentos que detalhem o funcionamento do processo de concessão e retirada de acessos (meios de comunicação utilizados, formulários, armazenamento das informações, padrões de nomenclatura utilizados, entre outros aspectos).

DEFINIÇÃO DE RESPONSABILIDADES
A concessão de acessos aos sistemas em utilização na DPE/BA é de competência da área gestora.

GESTÃO DOS ACESSOS (CONCESSÃO, TRANSFERÊNCIA E EXCLUSÃO)
É de responsabilidade da unidade requisitante, solicitar ao(à) responsável pelo processo de negócio ou sistema a inclusão ou alteração dos perfis de acesso do mesmo. Para decidir sobre a aprovação ou não das solicitações, o(a) responsável pelo processo de negócio ou sistema deverá avaliar a solicitação com base nas responsabilidades e atividades desempenhadas pelo requisitante.
Todos os membros, servidores(as) e demais colaboradores(as) deverão utilizar, obrigatoriamente, o mesmo processo de concessão de acesso para obter uma conta de acesso aos sistemas de informação.
Qualquer solicitação de acesso deverá ser feita através de chamado via servicedesk.
As contas de acesso pertencentes a prestadores(as) de serviços e visitantes deverão ser bloqueadas ao término de seus projetos, ou período de prestação de serviço, sendo que essa data deverá ser definida pela área solicitante.
Caso o(a) terceiro(a) pare de prestar serviços para a DPE/BA antes do período previsto, é dever do(a) fiscal do contrato comunicar à Central de Serviços, via abertura de chamado, que determinado(a) terceiro(a) já não presta mais serviços para a DPE/BA e, portanto, já não necessita mais dos acessos.
Enquanto a área responsável não notificar o desligamento do(a) terceiro(a) ou prestador de serviço, o acesso será mantido e as responsabilidades atribuídas para o(à) usuário(a) em questão permanecerão com a área solicitante.
Cabe à área responsável comunicar através de chamado na Central de Serviço, para evidenciar a referida comunicação em tempo hábil, sobre os desligamentos de membros, servidores(as) ou eventuais colaboradores(as) ocorridos, para que a Central de Serviço efetue as devidas exclusões dos acessos à rede/sistemas acessados.
É de responsabilidade da área responsável notificar através de chamado na Central de Serviço que determinado membro, servidor(a) ou eventual colaborador(a) foi transferido(a) de uma área para outra.

APROVAÇÃO
As solicitações de criação de usuários e alterações de perfis de acesso deverão passar, obrigatoriamente, pela aprovação do(a) gestor(a) da unidade do(a) usuário(a) requisitante. Os pedidos de aprovação serão enviados através do sistema de servicedesk. O(a) gestor(a) receberá as notificações de aprovação por e-mail. Serão enviados até três (03) pedidos de aprovação. Se nenhum deles forem respondidos os acessos não serão concedidos e o chamado encerrado.

RETIRADA PARCIAL DE ACESSOS
A retirada parcial dos acessos poderá ocorrer sempre que um membro, servidor(a) ou eventual colaborador(a) tiver suas atividades diárias alteradas ou então quando determinada responsabilidade ou módulo de acesso não for mais necessário para seu trabalho.

REGRAS GERAIS DE ACESSO
Não será permitido, em hipótese alguma, o compartilhamento das contas de acesso entre os(as) usuários(as) dos sistemas de informação. Quaisquer exceções deverão ser verificadas pela Área de Segurança da Informação.
Não será permitida a existência de usuários do tipo "genérico" cadastrados nos ambientes de produção dos sistemas de informação, ou seja, contas de acesso que não possuem um(a) responsável único(a), salvo após aprovação da área de Segurança da Informação, que providenciará a aprovação para criação desta conta.
Todas as contas de acesso devem possuir um(a) único(a) responsável (membro, servidor(a), colaborador(a), prestador(a) de serviço ou visitante), com indicação de seu nome completo (nome e sobrenome).
Não são permitidas contas de usuários(as) prestadores(as) de serviço ou de visitantes com direitos de administração nos ambientes de produção de qualquer

sistema de informação, a menos que sejam prestadores(as) de serviços da CMO e que sejam devidamente autorizados(as) pelo(a) responsável da área.

REVISÃO DE ACESSOS
A área de Segurança da Informação deverá analisar periodicamente os acessos ativos dos sistemas de informação.
Os sistemas que são revisados são definidos pela Área de Segurança da Informação de acordo com a criticidade de cada um. Os Usuários de rede (Active Directory) também são revisados periodicamente.
É importante ressaltar que essa revisão não leva em conta os perfis de acesso de cada usuário(a), levando em conta apenas os acessos ativos.
Tal revisão será realizada ao menos uma (01) vez por ano, para cada sistema definido, de acordo com calendário estabelecido pela Coordenação de Modernização e Informática.
Ao fim de cada revisão, um relatório será criado pela área de Segurança da Informação e será enviado para as áreas responsáveis pela concessão de acesso aos sistemas.
Se durante o trabalho de revisão forem encontrados acessos indevidos, os mesmos poderão ser bloqueados imediatamente, sendo liberados após regularização, se for o caso.

REVISÃO DOS PERFIS DE ACESSO
Os perfis de acesso aos sistemas de informação da DPE/BA devem estar condizentes com as atribuições de cada usuário(a), respeitando as melhores práticas de segregação de função, evitando assim, conflitos de interesses. Essa medida visa proteger os registros dos(as) usuários(as) nos sistemas utilizados pela instituição, garantindo que apenas pessoas autorizadas possam acessar e alterar as informações.
A revisão dos perfis deve ser realizada anualmente, sendo o(a) responsável por essa atividade o(a) gestor(a) aprovador(a) de cada sistema/módulo.
Caso em alguma das revisões seja necessária alguma modificação nos perfis/acessos, a área de Segurança da Informação da CMO será responsável por providenciar o chamado para que a alteração solicitada seja realizada.

PRIVILÉGIOS ADMINISTRATIVOS
As contas de acesso privilegiado a sistemas corporativos, equipamentos de redes e sistemas operacionais, devem ser restritas aos(às) funcionários(as) da CMO que não consigam desempenhar suas funções diante da instituição, sem que tal tipo de acesso seja concedido.

ACESSO EM BANCO DE DADOS
O acesso direto a banco de dados em ambientes produtivos, por parte de servidores(as) ou eventuais colaboradores(as) que não fazem parte da CMO não é permitido, tanto para consulta, quanto para edição de dados. Eventuais exceções deverão ser formalizadas e aprovadas pelo(a) responsável da área solicitante e pela CMO.

BACKUP
A frequência e periodicidade de realização dos backups devem ser definidas conforme a necessidade do negócio, a criticidade da informação para a continuidade das operações, requisitos de segurança e de auditoria.
As mídias de backup devem ser armazenadas em local distante do datacenter principal que ofereça proteções contra alta temperatura, umidade e acessos não autorizados.

UNIDADES COM SISTEMA DE BACKUP GERENCIADO
- Sede Administrativa (CAB) Unidade de Atendimento (Canela)
- Casa de Acesso à Justiça I (Jardim Baiano) Casa das Famílias I e II (Jardim Baiano)
- 1ª DPE Regional (Feira de Santana)
- 2ª DPE Regional (Vitória da Conquista)

Os backups deverão ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

MANUSEIO E TRANSPORTE DAS MÍDIAS DE BACKUP
O transporte das mídias de backup até o local de armazenamento remoto, quando ocorrer, deve ser realizado de forma adequada e segura, garantindo o acondicionamento correto das mídias e a proteção adequada contra acessos indevidos, danos, perda ou roubo.
Toda e qualquer movimentação de mídias entre sites deve ser documentada, através de controle próprio, detalhando dia, hora e responsável pela movimentação.

ARMAZENAMENTO DAS MÍDIAS DE BACKUP
O local de armazenamento das mídias de backup deve possuir segurança física, de acordo com as necessidades do negócio, a criticidade das informações e os riscos previamente avaliados, a fim de garantir a proteção contra acessos indevidos e danos que possam comprometer a confidencialidade, integridade e disponibilidade das informações armazenadas;
As mídias de armazenamento utilizadas para rotinas de backup devem ser adequadas aos equipamentos utilizados para realização de backup.
A CMO é responsável pela execução dos procedimentos descritos nesta política e deverão prover regularmente a relação com os tipos de mídias (temporárias ou de retenção), utilizados para execução dos backups.
As mídias de backup devem estar armazenadas sob níveis de temperatura e umidade adequados, conforme as recomendações do fabricante. Elas também não devem ser submetidas ou armazenadas nas proximidades de campos magnéticos.

TESTES DE INTEGRIDADE
Semestralmente a equipe da CMO deverá realizar testes de Recuperação de Dados por amostragem, com o objetivo de atestar a integridade e disponibilidade dos dados armazenados.
A recuperação deve ser integral de pelo menos um servidor/sistema escolhido aleatoriamente, e deve ser planejada e documentada para fins de auditorias futuras.

REGISTRO DE FALHAS
As falhas referentes a problemas com o processo de backup e restore de informações devem ser registradas e reportadas.
Os registros de falhas devem ser avaliados para assegurar que as mesmas foram satisfatoriamente resolvidas, e as medidas corretivas aplicadas pós-falhas foram documentadas no chamado.

RESTORE DOS DADOS
A restauração das cópias de backup deve ser realizada através da abertura de chamado com a aprovação do(a) proprietário(a) da informação.
Para casos relacionados a incidentes com servidores, fica a critério da CMO avaliar a necessidade de recuperação, a fim de restabelecer o ambiente o mais rápido possível.

SUBSTITUIÇÃO E DESCARTE DE MÍDIAS
Todas as mídias fixas ou removíveis devem possuir descartes seguros.
As mídias de backup devem ser utilizadas somente durante o tempo de vida útil especificado pelo fabricante. Após o término deste período, a mídia deve ser substituída e descartada.
Em caso de dano ou alerta de mídia degradada ou com risco de defeito pela ferramenta de backup, essa mídia deve ser substituída e posteriormente descartada.
As mídias devem ser destruídas adequadamente antes de serem descartadas, através de trituração, fragamentação mecânica, ou desmagnetização, de forma que os dados não possam ser recuperados, a fim de evitar o vazamento de informações confidencias e críticas para o negócio.
Todas as mídias descartadas devem ser registradas, de forma a manter uma trilha de auditoria.

OUTROS BACKUPS
Ao menos mensalmente deve ser realizada pela equipe de infraestrutura da CMO uma cópia do arquivo de configuração dos equipamentos (ex.: switches, firewall, etc.), e esse arquivo deve ser armazenado em local seguro.

BACKUP NÃO AUTOMATIZADO E NÃO GERENCIADO
Em unidades cujo serviço de backup gerenciável ainda não foi implementado, os(as) usuários(as) deverão realizar periodicamente cópias de segurança das informações, pois os discos rígidos dos computadores são passíveis a falhas mecânicas ou lógicas.
Arquivos excluídos de forma acidental por usuários(as) não poderão ser restaurados através de dispositivos de backup.

GERENCIAMENTO DE LOGS
Todos os sistemas operacionais, sistemas de aplicativos e equipamentos de redes devem ser devidamente configurados para que gerem logs de eventos, segurança e auditoria.
Todos os equipamentos devem gerar seus logs em um servidor centralizado, para evitar o risco de adulteração dos logs, e para que seja possível realizar a correlação dos eventos.

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
Um Incidente de Segurança da Informação pode ser detectado de várias maneiras, como por exemplo, através dos logs dos servidores, dos ativos de rede, do firewall, dos desktops, dos sistemas de informação, entre outros. A detecção também pode ocorrer após contato de algum(a) usuário(a) dos sistemas de informação que identificar uma situação atípica no ambiente, realizando uma denúncia para a equipe de TI, seja via abertura de chamado, e-mail, contato telefônico ou mesmo pessoalmente.
É dever de todo membro, servidor(a) ou eventual colaborador(a) comunicar ao Service Desk a identificação de um incidente de segurança da informação, ou a suspeita de que um incidente esteja em curso, para que sejam realizadas as análises necessárias e as medidas adequadas sejam tomadas.
É de responsabilidade do CMO a implantação de uma equipe de resposta a

incidentes de Segurança da Informação, de forma que as fragilidades e eventos de segurança associados aos ativos de informação sejam comunicados ao Comitê de Segurança da Informação e aos Encarregados de Proteção de Dados, permitindo a tomada de ação corretiva em tempo hábil e com a orientação de preservar ou restabelecer operantes os recursos de TIC oferecidos.
A CMO tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TIC, sobretudo em casos de incidente de Segurança de Informação.

GERENCIAMENTO DE RISCOS
A Coordenação de Modernização e Informática – CMO deve mapear, documentar, e comunicar ao Comitê de Segurança da Informação e aos Encarregados de Proteção de Dados as ameaças e vulnerabilidades que redundam em risco ao negócio e à infraestrutura de tecnologia que o suporta, pare que busquem a solução adequada para cada caso.

PLANO DE CONTINUIDADE
É de responsabilidade do Comitê de Segurança da Informação coordenar a elaboração, execução, teste e renovação de plano que tenha como objetivo minimizar o impacto na disponibilidade dos recursos críticos de TIC e, consequentemente, nos processos da DPE/BA por eles suportados.
É de responsabilidade do Comitê de Segurança da Informação aprovar a estratégia de continuidade do plano e fornecer subsídios para a sua implementação.
Independentemente da existência de um plano de continuidade dos negócios ou de recuperação a desastres, a CMO deve estabelecer normas e procedimentos para backup, com frequência de realização diária, mantendo sempre a base de dados tão atualizada quanto possível.

GLOSSÁRIO
Antivírus - programa que permite identificar e eliminar vírus em computadores.
Autenticação - é um processo que busca verificar a identidade digital do(a) usuário(a) de um sistema no momento em que ele(a) requisita acesso em um programa ou computador.
Ativo - tudo aquilo que tem valor tangível ou intangível, como informações, sistemas de informação, equipamentos, serviços, imagem institucional e processos internos.
Backup - é a cópia de segurança de um conjunto qualquer de dados. É realizada copiando-se os dados de um dispositivo de armazenamento de origem para outro, de destino.
Bancos de dados - conjunto de dados inter-relacionados, representando informações sobre um domínio de informação específico.
Chamado - é um registro de informação que evidencia uma demanda de usuário(a), bem como as tratativas que lhe foram dadas. Cada chamado possui um número único.
Custodiante - qualquer pessoa física ou jurídica, que detenha a posse de informação produzida por outrem.
Download - transferência de dados de um computador remoto para um computador local.
Estação de Trabalho - equipamento utilizado pelo(a) usuário(a) para desenvolver suas tarefas. Pode ser um notebook, computador de mesa, etc.
Hardware - parte física do computador, ou seja, é o conjunto de componentes eletrônicos.
Incidente de segurança - qualquer evento, confirmado ou sob suspeita, que gere dano ou ameace a integridade, confidencialidade, disponibilidade e autenticidade das informações.
Login - identificação do(a) usuário(a) perante os sistemas de informação, de caráter pessoal, intransferível.
Logoff - término no uso de um sistema computacional.
Logon - identificação do(a) usuário(a) juntamente com a palavra chave para início do uso de um sistema computacional.
Malware - termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, worms, bots, cavalos de tróia, spywares, rootkits, etc.
Restore - procedimento utilizado para restaurar no devido ambiente o conteúdo de uma cópia de segurança, recuperando assim os dados anteriormente armazenados.
Senha de Acesso - também denominada Senha ou Password. É um código secreto que o(a) usuário(a) precisa apresentar para ser validada em um processo de autenticação.
Servidor - computador que fornece serviços ou recursos para outros computadores.
Spam - termo empregado para referir-se aos e-mails não solicitados, que geralmente, mas não necessariamente, são enviados para um grande número de pessoas.
Storages - hardware que contém espaços para vários discos rígidos, conectado aos servidores, a fim de armazenar os dados com segurança.
Software/Aplicativo - programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador ou sistema de processamento de dados. Exemplos: sistemas operacionais, software de projetos, software de editoração gráfica/desenhos, softwares de rede, editor de texto, planilha de cálculo, software de apresentação, antivírus, antispam, drivers, firmware, correio eletrônico e aplicativos em geral.
Switch - é um equipamento que interliga os computadores em uma rede.
Upload - referente à ação de enviar dados de um computador local para um computador ou servidor remoto, geralmente através da internet.
Usuário(a) - toda e qualquer pessoa que tenha acesso aos ativos de informação da Defensoria Pública, direta ou indiretamente.
VPN - Sigla para Virtual Private Network (Rede Virtual Privada). É uma tecnologia para criptografar os dados que são transferidos entre duas ou mais redes em uma estação de trabalho, homologado.
Referências
https://www.justicaeleitoral.jus.br/arquivos/tre-mg-resolucao-tre-mg-n-945-de-17-de-dezembro-de-2013/rybena_pdf?file=https://www.justicaeleitoral.jus.br/arquivos/tre-mg-resolucao-tre-mg-n-945-de-17-de-dezembro-de-2013/at_download/file
http://www.fortic.ba.gov.br/index.php/download/seguranca-da-informacao?download=57:normas-deseguranca-da-informacao-do-estado-da-bahia
https://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf
http://www7.tj.ba.gov.br/secao/lerPublicacao.wsp?tmp.mostrarDiv=sim&tmp.id=22913&tmp.secao=9
https://www.sebraepr.com.br/wpcontent/uploads/Politica_de_Seguranca_da_Informacao_e_Comunicacao.pdf
http://defensoria.pe.def.br/defensoria/sites/defensoriape//pdf/Pol_de_Seg_da_Informacao_DPPE.pdf

Defensoria Pública BAHIA