Tribunal de Justiça do Estado da Bahia

Sistema de Publicação de Conteúdo

DECRETO JUDICIÁRIO Nº 251, DE 27 DE MAIO DE 2019.

DISPONIBILIZADO NO DIÁRIO DA JUSTIÇA ELETRÔNICO NO DIA 28 DE MAIO DE 2019.

Implementa a Política de Segurança da Informação e institui Normas para Utilização de Recursos de Tecnologia da Informação, para Gestão de Ativos, de Classificação de Informações, de Gerenciamento de Acessos, de Gestão de Operação de Tecnologia da Informação, de Desenvolvimento Seguro, de Gerenciamento de Riscos de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado da Bahia.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução nº 211-CNJ, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário;

CONSIDERANDO a Resolução nº 6, de 7 de maio de 2014, que instituiu no âmbito deste Poder a Política de Segurança e Sistema de Segurança da Informação – SSI, na forma do Anexo II da referida Resolução;

CONSIDERANDO o disposto no item 17.3, Anexo I, e nos itens 13.5, 13.6, 13.7, do Anexo II, da Resolução nº 6/2014;

CONSIDERANDO o disposto na Resolução nº 14, de 31 de agosto de 2016, que instituiu o Comitê Gestor de Segurança da Informação,

CONSIDERANDO que compete ao Comitê Gestor de Segurança da Informação elaborar e manter a política de Segurança da Informação, propondo as normas e procedimentos de Segurança da Informação do Poder Judiciário do Estado da Bahia que garantam a disponibilidade, a integridade, a autenticidade e o sigilo de dados, entre outros; e

CONSIDERANDO o que consta do expediente TJ-COI-2018/10028, e a manifestação da Comissão Permanente de Segurança,

RESOLVE

Art. 1º Implementar, no âmbito do Poder Judiciário do Estado da Bahia, a Política de Segurança da informação na forma do Anexo I.

Art. 2º Instituir as Normas para Utilização de Recursos de Tecnologia da Informação, para Gestão de Ativos, de Classificação de Informações, de Gerenciamento de Acessos, de Gestão de Operação de Tecnologia da Informação, de Desenvolvimento Seguro, Norma de Gerenciamento de Incidentes de Segurança e de Gerenciamento de Riscos de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado da Bahia na forma dos Anexos II, III, IV, V, VI, VII, VIII e IX, respectivamente.

Art. 3º Para melhor entendimento dos Anexos utilizou-se as definições constantes do Anexo X – Glossário.

Art. 4º Este Decreto entra em vigor na data de sua publicação, ficando revogadas disposições contrárias.

Art. 5º Os casos omissos serão resolvidos pela Presidência do Tribunal de Justiça da Bahia.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, em 27 de maio de 2019.

Desembargador GESIVALDO BRITTO

Presidente

ANEXO I – Política de Segurança da Informação

I- Disposições Gerais

1.1. O Comitê Gestor de Segurança da Informação e a Secretaria de Tecnologia da Informação e Modernização, observados os princípios da confidencialidade, disponibilidade, integridade, legalidade e autenticidade, em complemento às disposições da Resolução nº 6/2014, no que pertine à segurança da informação, desenvolverá e implementará os processos e métodos necessários para e suficientes para:

1.1.1. Gerir os riscos da ocorrência de eventos que possam causar danos às pessoas, ao patrimônio e às informações, relativos à atuação institucional, prevenindo-os ou, pelo menos, reduzindo-os a níveis mínimos aceitáveis; e

1.1.2. Minorar os impactos de situações anormais de funcionamento que afetem a confidencialidade, disponibilidade, integridade, legalidade e autenticidade das informações, caso ocorram.

1.2. A Política de Segurança da Informação alcançará todas as unidades do Poder Judiciário do Estado da Bahia de acordo com as seguintes diretrizes:

1.2.1. Gestão permanente da segurança provendo os recursos físicos, tecnológicos e ambientais adequados para a manutenção desta política, racionalizando os custos e minimizando os riscos;

1.2.2. Cooperação entre as unidades do Tribunal de Justiça do Estado da Bahia, bem como entre os conveniados, contratados, demais órgãos e Poderes públicos, promovendo o intercâmbio científico-tecnológico e de informações relativas a eventos de risco e a segurança orgânica;

1.2.3. Padronização de processos e soluções, assegurando a interoperabilidade entre os sistemas de informação;

1.2.4. Otimização da alocação de recursos e tecnologias nos vários níveis da segurança orgânica por meio da gestão de riscos de Segurança;

1.2.5. Elaboração e implementação de programas de conscientização e capacitação que se fizerem necessários para a efetiva implantação desta Política de Segurança, com a fiel observância a seus dispositivos, normativos e demais procedimentos complementares; e

1.2.6. Adoção consistente e racionalizada de tecnologias de segurança.

1.3. A Política de Segurança da Informação obriga a todos os colaboradores, que ficam cientes das práticas definidas nas normas vinculadas a este documento, práticas estas que regulam os assuntos relacionados à utilização dos equipamentos e dos Sistemas de Informação do TJBA e demais sucursais.

1.3.1. O colaborador do TJBA que, intencionalmente, violar esta Política de Segurança da Informação responderá pela infração cometida, ficando sujeito a sanções disciplinares.

1.4. O descumprimento desta Política de Segurança por prestadores de serviços devidamente contratados para a execução de serviços variados em Tecnologia da Informação será classificado como motivo de quebra do Contrato de Prestação de Serviços, independentemente de medidas judiciais cabíveis nas esferas penal, cível e administrativa.

1.5. O Tribunal de Justiça do Estado da Bahia adotará as medidas cabíveis contra qualquer pessoa física ou jurídica que venha a praticar atos que violem a Política de Segurança estabelecida neste documento e demais Anexos.

1.6. Os recursos de informática disponibilizados pelo TJBA são fornecidos com o propósito único de garantir o desempenho das atividades de cada colaborador, 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.

1.7. Os recursos de TIC (Tecnologia da Informação e Comunicação) utilizados no TJBA podem ser gerenciados, monitorados e auditados periodicamente pelo responsável do Departamento de Auditoria Interna, objetivando verificar a correta implementação dessa Política e seus anexos.

II - Dos papéis e responsabilidades

2. É papel:

2.1. De todo colaborador conhecer e seguir as regras definidas nesta Política de Segurança da Informação, sob pena de responsabilização em caso de descumprimento da mesma e possível sanção disciplinar.

2.2. De todo gestor ter postura exemplar em relação à Segurança da Informação e disseminar as boas práticas definidas pelo TJBA em sua área de atuação, sendo de sua responsabilidade gerir os acessos de seus colaboradores nos sistemas de informação da instituição, a fim de minimizar riscos de que acessos indevidos ocasionem vazamentos de informação.

2.3. Do Comitê Gestor 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 no TJBA.

2.3.1. Também é papel do CGSI definir e gerir processos de Segurança da Informação, propor investimentos e projetos em Segurança da Informação, propor alterações e aprovar a Política de Segurança da Informação, bem como seus documentos complementares, sem prejuízo das atribuições estabelecidas na Resolução nº 14, de 31 de agosto de 2016.

2.4. Da Secretaria de Tecnologia da Informação e Modernização 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 elaborar minutas de normativo técnico complementar a este documento e demais Anexos quanto ao quesito da segurança da informação.

2.5. Da Diretoria de Informática garantir que os sistemas e ambiente tecnológico utilizados pelos colaboradores e usuários dos sistemas e equipamentos do TJBA forneçam proteção adequada às informações durante todo o seu ciclo de vida (criação, armazenamento, uso, transferência, arquivamento e descarte).

2.6. Dos Gestores e Fiscais dos contratos de prestação de serviço o registro e manutenção, no sistema de controle de acesso, dos dados dos funcionários vinculados aos respectivos contratos.

2.7. Da Secretaria de Administração do Tribunal de Justiça do Estado da Bahia o apoio técnico e operacional no planejamento estratégico da segurança institucional, cabendo-lhe, ainda:

2.7.1. Elaborar e executar os projetos de construção e reforma para adequação das unidades dos quesitos de segurança orgânica;

2.7.2. Articular as unidades envolvidas no processo, com vistas à eficiência nas atividades administrativas e operacionais;

2.7.3. Gerir os contratos de serviços necessários à implantação e funcionamento do controle de acesso, vídeo monitoramento, vigilância e recepção;

2.7.4. Cadastrar e fornecer os cartões de acesso destinados a estagiários e prestadores de serviço cujas emissões foram solicitadas pelas unidades gestoras dos respectivos contratos e criar diretrizes para permissões de acesso de pessoas, veículos e materiais.

2.8. Do Gabinete de Segurança Institucional realizar o apoio técnico e operacional no planejamento estratégico da segurança institucional, atuando na supervisão do monitoramento de imagens, de acesso de pessoas, veículos e materiais e atuar nos estudos comportamentais de segurança, mediante análise de imagens de vídeo monitoramento e do fluxo de pessoas, além de outros meios que se fizerem necessários.

III - Do treinamento e conscientização

3. É de responsabilidade do Comitê Gestor de Segurança da Informação prover treinamento sobre Segurança da Informação a todos os colaboradores e realizar atividades pontuais para aumentar a conscientização com relação a este assunto.

3.1. Essas atividades podem ser realizadas através de cursos on-line EAD, mensagens eletrônicas disparadas periodicamente, notícias e dicas de utilização disponibilizadas na intranet, eventos anuais de Segurança da Informação, entre outras atividades.

3.2. A não realização dos treinamentos obrigatórios definidos pelo TJBA poderá ocasionar no bloqueio dos acessos à rede e sistemas em caso de não participação por parte dos colaboradores.

IV - Da revisão

4. Esta Política de Segurança da Informação e seus documentos complementares devem ser revisados criticamente ao menos 1 (uma) vez ao ano ou toda vez que houver uma alteração significativa no ambiente computacional ou organizacional.

4.1. A responsabilidade por iniciar a revisão é da área COTEC e do Comitê Gestor de Segurança da Informação que deve revisar e aprovar as modificações realizadas na documentação.

V - Da propriedade intelectual

5. Todo o conteúdo desenvolvido pelos colaboradores durante o horário do expediente, nas dependências do TJBA ou remotamente, com a finalidade de atender especificamente aos requisitos de negócio do TJBA é de propriedade do TJBA.

5.1. Estão incluídos nesses itens planilhas e fórmulas, formulários, fluxos de trabalho, código fonte de sistemas e aplicações, scripts de automação, etc.

Anexo II – Norma para Utilização de Recursos de Tecnologia da Informação

I - Da utilização de equipamentos

1.0. Todo o gerenciamento dos equipamentos e dos Sistemas de Informação do Tribunal de Justiça do Estado da Bahia é de responsabilidade da Secretaria de Tecnologia e Modernização (SETIM).

1.1. A responsabilidade pela conservação de cada equipamento é do colaborador que os utiliza diariamente, devendo ser evitada a presença de copos com líquidos próximos aos equipamentos, inclusive os notebooks, celulares ou smartphones, evitando, ainda colar adesivos nos equipamentos, pois eles poderão ser utilizados por outra pessoa futuramente.

1.2. O transporte dos equipamentos deve ser realizado em mochila ou mala apropriada, para evitar danos ao mesmo. Durante seu trânsito, o colaborador deverá ter o equipamento sempre consigo, não o deixando desacompanhado, seja no carro, em ambientes externos, aeroportos, hotel, etc.

1.3. Nenhum equipamento deve ser deixado ligado ou desprotegido de senha no descanso de tela quando não estiverem em uso.

1.3.1. É de responsabilidade dos funcionários e prestadores de serviços que os utilizam assegurarem o cumprimento desse requisito.

1.3.2. 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. Caso o procedimento acima não seja realizado, as estações serão automaticamente bloqueadas após 5 minutos de inatividade.

1.4 Não é permitido instalar softwares sem o conhecimento da DIN. Toda necessidade de instalação de novo programa ou software deve ser formalizada via abertura de chamado para que possa ser devidamente analisada pela área e o software instalado, observando as regras internas e sem prejudicar a segurança da instituição como um todo.

1.5. A manutenção física dos equipamentos (adição, remoção e substituição de hardware) é de responsabilidade da DIN, sendo que é proibido aos colaboradores de outras áreas a execução dessas atividades.

1.6. Os equipamentos disponibilizados pelo TJBA a seus colaboradores são de uso exclusivamente profissional é restrito às atividades ligadas ao negócio da instituição, sendo proibido o uso particular.

1.7. É vedada a utilização de equipamentos para meios ilícitos, como por exemplo envio de material sexualmente explícito, com 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.

1.8. O colaborador deve 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.

II - Da proteção contra códigos maliciosos

2.0. 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 DIN, bem como a responsabilidade por instalar e manter a ferramenta antivírus operacional nos servidores e estações de trabalho.

2.1. É responsabilidade da DIN manter e gerenciar uma solução de antispam no ambiente de e-mail do TJBA, com a finalidade de filtrar e-mails indesejados e que contenham ameaças ao ambiente computacional da instituição.

2.2. Fora do ambiente computacional do TJBA o próprio colaborador é o responsável pela atualização do software de antivírus e execução de varredura em equipamento pertencente ao TJBA sob sua responsabilidade.

III - Da divulgação de informações

3.0. Todas as informações do TJBA, independente do formato em que se encontram (gravadas em meios magnéticos, impressas, entre outros), devem ser protegidas pelo proprietário da informação, de maneira proporcional ao seu grau de importância e classificação.

3.1. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada nos ativos de informação do TJBA, seja por seus funcionários ou terceiros, é considerada seu patrimônio e deve ser protegida conforme estabelecido na legislação vigente.

3.2. Não é permitido fornecer informações para nenhuma pessoa externa ou não à organização, a menos que seja mediante autorização expressa dos gestores envolvidos e que o solicitante esteja devidamente identificado e ainda possua uma justificativa válida de negócio.

3.3. 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.

3.4. 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.

3.5. Arquivos, documentos e mensagens eletrônicas não mais necessários e/ou obsoletos deverão ser inutilizados e descartados.

IV - De contratos e acordos comerciais

4.0 Nenhuma atividade que envolva a contratação de prestadores de serviço (que envolverem 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.

4.1. Os contratos de serviços de terceiros devem ser validados sob os aspectos técnico, operacional e comercial, pelos responsáveis pela contratação, de acordo com os padrões do TJBA.

4.2. Todos os contratos com os prestadores de serviço devem conter cláusula específica de sigilo e confidencialidade em relação a toda e qualquer informação do TJBA a que este prestador tenha acesso.

4.3. 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 pelo TJBA, todos os artefatos produzidos, inclusive código-fonte, no escopo deste contrato, pertencerão ao TJBA, não sendo possível sua divulgação ou reutilização externa, salvo autorização expressa do TJBA.

V - Dos dispositivos de armazenamento externo

5.0. Os usuários 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 podendo danificar e corromper dados, assim como, o vazamento de informações corporativas confidenciais.

5.1. Seu uso exige cautela, para reduzir o risco tanto de vazamento de informações internas quanto o comprometimento do equipamento/rede através de softwares maliciosos. Para obter maiores informações a respeito da utilização segura desse tipo de mídia, os colaboradores devem entrar em contato com a DIN, para correta orientação.

5.2. Ao encontrar algum pendrive ou mídia removível perdido pelas dependências do TJBA, a instrução é que o mesmo seja levado até a DIN para análise prévia.

VI - Do acesso remoto

6.0. O padrão para permitir que colaboradores se conectem remotamente nas redes do TJBA é a VPN (Virtual Private Network). Nenhuma outra forma de acesso remoto é permitida.

6.0.1. A utilização desse recurso requer um acesso à Internet, fazendo com que sua conexão à internet seja estabelecida antes de se conectar à VPN do TJBA. Como o usuário 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 o TJBA. Uma vez conectado à VPN, o usuário deverá acessar apenas o recurso de destino para o qual o acesso foi designado.

6.0.1.1. Os métodos de conexão à VPN e os grupos de colaboradores a quem se destina cada método são definidos pela DIN e podem variar de acordo com a tecnologia utilizada.

6.0.1.2. O colaborador que dispõe de acesso à VPN não pode, em hipótese alguma, compartilhar seu usuário e senha com outras pessoas.

6.0.2. O TJBA possui a autonomia de bloquear o acesso de um determinado usuário 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.

VI.1- Do acesso remoto para funcionários

6.1. O colaborador pode requerer acesso remoto à VPN do TJBA uma vez que identifique a necessidade de se atuar com ferramentas ou acessar informações presentes apenas internamente na instituição, sendo que ele se encontra fisicamente fora das dependências da instituição.

6.1.1. Este acesso requer a aprovação formal de seu superior e as regras para este tipo de atuação seguem as mesmas regras de quando o colaborador está atuando localmente em seu ambiente de trabalho usual (dentro das dependências da instituição).

6.1.2. Desde que se comprove a real necessidade e que haja possibilidade da DIN, é recomendado testar a configuração previamente, junto com o usuário que irá utilizar.

VI.2- Do acesso remoto para prestadores de serviços

6.2. O prestador de serviços pode utilizar o acesso remoto desde que o responsável da área solicitante do acesso, em conjunto com o responsável da área de Segurança da Informação, aprove essa utilização.

6.2.1. Todas as regras de segurança impostas aos colaboradores do TJBA devem ser seguidas pelo prestador de serviço quando conectado à VPN.

6.2.2. Uma vez conectado à VPN, o prestador de serviço deverá acessar apenas o recurso de destino para o qual o acesso foi designado e para o qual ele foi contratado.

6.2.3. No ato da concessão do acesso, a área deve definir o prazo que o acesso remoto se manterá vigente. Este prazo não poderá ser maior que 30 dias além do prazo para o término do projeto (reservado para acompanhamento quando houver necessidade). Além disso, apenas os recursos necessários deverão ser liberados para o terceiro, não sendo permitido o uso irrestrito dos recursos computacionais remotamente.

6.2.4. Não é permitido, para prestadores de serviço, o acesso à VPN de suas respectivas empresas, partindo de dentro das dependências do TJBA.

6.2.5. Não é permitido, em hipótese alguma, o compartilhamento do usuário de VPN entre os prestadores de serviço.

6.2.6. Terceiros e prestadores de serviço que realizarão somente trabalhos remotos (ex: consultorias de outros estados), deverão seguir as mesmas normas e recomendações para os funcionários internos.

6.2.7. O acesso somente será concedido após o contrato entre a consultoria e o TJBA tiver sido firmado, contendo uma cláusula de confidencialidade, impedindo a divulgação das informações por ambas as partes.

VI.3- Do acesso via VPN entre empresas

6.3. O TJBA pode estabelecer VPN no modelo "site-to-site" entre empresas e outros órgãos públicos, desde que seja acordado um padrão de configuração que forneça segurança o suficiente para a comunicação, compatível com as regras de negócio e requisitos técnicos.

6.3.1. O TJBA não se responsabiliza por garantir desempenho em conexões VPN, uma vez que esta conexão depende de configurações e requisitos de infraestrutura aos quais o TJBA não tem autonomia.

VI.4- Do suporte

6.4. O suporte à VPN é realizado pela equipe de suporte da DIN, oferecido no modelo comum de trabalho, em horário comercial, através de telefone e de chamado na ferramenta oficial do TJBA.

VII - Do uso de credenciais de acesso

7.0. 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.

7.0.1. Diante do grau de importância deste mecanismo, para que consigamos um nível adequado de controle, devemos prezar pela guarda desta credencial.

7.0.2. Algumas recomendações referentes à composição e uso de senhas de acesso, com o objetivo de assegurar sua confidencialidade:

a) Recomenda-se que a senha seja trocada imediatamente após o primeiro acesso. Depois disso, a troca deve ser efetuada mediante solicitação automática do sistema;

b) Recomenda-se que seja composta por, pelo menos, 8 (oito) caracteres. É importante ressaltar que, quanto maior a senha, maior a dificuldade em decifrá-la;

c) 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;

d) 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);

e) Não utilize senhas contendo o termo “TJ”, “TJBA”, etc., pois são fáceis de serem adivinhadas ou decifradas;

f) A senha deve ser imediatamente alterada caso desconfie ou tenha indícios de que tenha sido decifrada;

g) Evite reutilizar senhas antigas;

h) Não se deve guardar anotações de senhas em blocos de anotações, post-it nos monitores, embaixo dos teclados, anotado no calendário, em baixo do aparelho telefônico, agendas ou qualquer local de fácil acesso;

7.0.3. Cada usuário 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 colaborador 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;

7.0.4. Contas de acesso à rede devem ser individuais e não compartilhadas, salvo em situações especiais em que a DIN julgar necessárias e dentro de prazos curtos e predeterminados;

7.0.5. Os sistemas que possuírem métodos de configuração de senha forte, terão essas configurações implementadas. Caso contrário, esse sistema será tratado como exceção pela DIN.

VII.1- Do envio de senhas

7.1. Após a criação de uma nova conta ou solicitação de nova de senha, esta deverá ser enviada diretamente ao usuário, seguindo as regras abaixo:

7.1.1. Se for a senha do usuário de rede ou conta de e-mail (tanto para uma nova conta quanto nova senha), deverá ser informada por notificação por e-mail para o superior imediato, ou seu representante devidamente autorizado.

7.1.8. Se for servidor, para os demais sistemas, a senha deverá ser enviada diretamente para o e-mail corporativo do funcionário. Para funcionários terceiros, a senha deverá ser enviada para o e-mail corporativo do funcionário na empresa que o mesmo trabalha.

7.1.9. Para empresas terceiras que não possuírem domínio próprio, o envio para contas de e-mail particular é permitido, desde que o nome da conta de e-mail esteja relacionado com o nome da empresa (ex. empresaxyz@gmail.com) e exista um contrato assinado entre o TJBA e a contratada.

VIII - Do uso de correio eletrônico

8.0. O e-mail 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 DIN.

8.0.1. A conta de correio (e-mail) é individual, não podendo ser compartilhada com outros funcionários. Os eventuais casos especiais deverão ser devidamente analisados.

8.0.2. O endereço de e-mail deverá ser formado pela inicial dos primeiros nomes e o sobrenome completo do colaborador. No caso onde já houver um endereço de e-mail com essa formatação, outras opções deverão ser analisadas pelas áreas responsáveis pela criação da conta de e-mail.

8.0.3. Nos casos das contas departamentais, um usuário deverá ser o responsável formal por realizar as manutenções nessa caixa de entrada, gerenciando o espaço disponível. Esse usuário também é responsável pelo conteúdo das mensagens recebidas e enviadas.

8.0.4. Para terceiros e prestadores de serviço, a formatação do e-mail deverá conter o nome da empresa e o nome do terceiro, criando assim, uma diferenciação entre os servidores e contratados terceirizados.

VIII.1-Das restrições no uso de correio eletrônico

8.1. Assuntos particulares não devem ser enviados por e-mail.

8.2. O envio de mensagens com destino a todos os usuários somente deve ser utilizado se o assunto for relacionado diretamente aos negócios da instituição e se realmente todos devem receber aquela mensagem;

8.3. 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 do TJBA 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;

8.4. 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.

8.5. A DIN pode definir os tipos de arquivos que podem ou não ser anexados/recebidos em um e-mail;

8.6. Não adicionar contas particulares através dos serviços POP, IMAP e SMTP de provedores não pertinentes ao domínio “@tjba.jus.br” aos clientes de e-mail utilizados na instituição;

8.7. A utilização de webmails particulares por parte dos colaboradores do TJBA não é proibida, porém, todo e qualquer assunto relacionado às atividades exercidas no TJBA deve ser tratado exclusivamente pelo endereço de e-mail corporativo.

8.8. Na necessidade de enviar um e-mail com documento confidencial para terceiros (que não utilize domínio “@tjba.jus.br”), o arquivo confidencial deve ser gerado compactado e com senha. A senha do arquivo compactado deve ser enviada em outra mensagem sem relação com o primeiro e-mail enviado.

IX - Do uso da internet

9.0. Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e utilizar seus recursos;

9.0.1. A Internet é um meio de comunicação de uso exclusivo para trabalhos da instituição.

9.0.2. A responsabilidade de liberação destes acessos cabe ao responsável da área requisitante, que deverá avaliar a necessidade e solicitar a DIN através de chamado.

9.0.3. Qualquer funcionário que tenha acesso a um computador e a rede, poderá utilizar a Internet desde que tenha a devida aprovação do seu superior.

9.0.4. Os níveis de acesso são definidos pela DIN e as categorias de sites permitidos e bloqueados em cada categoria também.

9.0.5. 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.

9.0.6. A utilização da rede INTERNET dentro da instituição deve obedecer aos seguintes critérios:

9.0.7. Todo acesso à Internet deve ser feito utilizando equipamentos e métodos de acesso providos e autorizados pela TJBA. Seu uso deve ser relacionado somente para fins que estejam diretamente ligados ao negócio da instituição;

9.0.8. É vedado o acesso a internet utilizando equipamentos corporativos através de modem particular;

9.0.9. O usuário deve 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 do TJBA, 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;

9.0.10. 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 é terminantemente proibido;

9.0.11. A DIN pode determinar quais os tipos de arquivo que podem ser copiados da internet para a rede interna, através de download;

9.0.12. 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 do TJBA;

9.0.13. 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 usuário pode solicitar o desbloqueio à DIN;

9.0.14. 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.

IX.1-Do uso de mídias sociais

9.1. O uso de redes sociais por parte dos colaboradores do TJBA deve ser restrito a assuntos profissionais. Não é permitido:

Divulgar informações de uso restrito ou confidenciais do TJBA nas Mídias Sociais;

Utilizar a logomarca e/ou nome do TJBA para se autopromover;

Divulgar ou retransmitir boatos ou rumores sobre o TJBA;

Participar de crises relacionadas ao TJBA nas Mídias Sociais;

Fazer comentários ofensivos, ou expor publicamente a situações vexatórias, colegas de trabalho (independente de hierarquia), parceiros, clientes, etc.

Levar discussões e debates sobre os acontecimentos do trabalho e/ou da empresa nas Mídias Sociais.

Utilizar o nome do TJBA em sua identificação pessoal (ex: perfil “Fulano TJBA” no Facebook, e-mail tjba_fulano@gmail.com etc.);

Inserir imagens das dependências do TJBA sem autorização;

Postar conteúdos que possam caracterizar discriminação racial, política ou de gênero como se fosse opinião do TJBA.

9.1.2. No caso de questionamentos sobre informações do TJBA, colaborador deverá orientar o interessado a entrar em com contato direto com a assessoria de imprensa da TJBA.

IX.2-Do uso de comunicadores instantâneos

9.2. A utilização de programas de comunicação como Skype, Google Talk, WhatsApp, Telegram, Yahoo Messenger e etc., de dentro das redes do TJBA, é liberada desde que solicitada e aprovada pelo superior do colaborador em questão.

X - Da utilização do servidor de arquivos

10. Todos os arquivos ou documentos institucionais do TJBA deverão estar armazenados em um diretório (pasta), disponibilizada pela DIN no servidor de arquivos disponibilizado pela DIN.

10.1. A criação e/ou manutenção desta pasta será efetuada mediante solicitação ao DIN através de chamado.

10.2. Todos os documentos armazenados no servidor de arquivos possuem cópia de segurança (backup).

10.3. 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 DIN. As solicitações de restauração de arquivos devem ser realizadas através da ferramenta de chamados e a DIN possui 48 horas para disponibilizar os arquivos restaurados.

10.4. O TJBA não se responsabiliza pelos documentos armazenados nos computadores/notebooks dos usuários.

10.5. A análise dos tipos de arquivos permitidos no servidor de arquivos é de responsabilidade da DIN, 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 DIN.

10.6. 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.

10.7. Caso após a remoção e compactação de arquivos, o espaço for insuficiente, a DIN deve ser contatada para avaliar as necessidades e possibilidades de aumento do espaço.

XI - Do uso de equipamentos portáteis

11.0. Não são permitidas alterações de configurações no hardware, no sistema operacional e de padrões dos aplicativos disponibilizados nos equipamentos cedidos para trabalho externo, estando o funcionário infrator sujeito as sanções disciplinares da Política de Segurança da Informação, bem como, responsabilizado pelos danos causados aos referidos equipamentos.

11.0.1. O equipamento cedido ao colaborador deve ser utilizado única e exclusivamente para execução das atividades relacionadas à empresa.

11.0.2. Quando em trânsito, ou qualquer outro lugar fora da empresa, o colaborador não deve emprestar, perder de vista ou deixar o equipamento sob a responsabilidade de terceiros.

11.0.3. Todas as informações armazenadas nos equipamentos são de propriedade do TJBA, não devendo, 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 negócio.

11.0.4. O TJBA reservará o direito de supervisionar todos os dados transmitidos/recebidos a partir destes equipamentos, não caracterizando quebra de sigilo, uma vez que os recursos colocados à disposição são de propriedade da mesma.

11.0.5. Em caso de falha em qualquer dispositivo do equipamento em questão, o usuário não deverá procurar assistência técnica ou fazer qualquer substituição de componentes (baterias, carregadores, antenas etc.) sem a autorização prévia da DIN.

11.0.6. Em caso de roubo, furto, perda total ou parcial do equipamento recebido, o usuário deverá comunicar imediatamente seu superior, a DIN e providenciar o registro de boletim de ocorrência (BO) junto à autoridade policial.

11.0.7 Todas as regras citadas acima valem para notebooks, celulares, smartphones, etc.

11.0.8. Não é permitida a utilização, pelos funcionários ou prestadores de serviço, de equipamentos e/ou componentes pertencentes ao TJBA fora das dependências da instituição sem prévia autorização formal (ex.: Termo de Responsabilidade para Utilização e Guarda de Equipamento Portátil).

11.0.9. Quando em viagem, os computadores portáteis devem ser levados como bagagem de mão.

XI.1- Do uso de equipamentos portáteis particulares

11.1. Funcionários que preferirem utilizar seus equipamentos particulares para fins institucionais só poderão fazê-lo com autorização explícita da área da DIN. 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 DIN.

11.2. Se após a análise o equipamento não estiver dentro dos padrões aceitáveis, a DIN poderá sugerir a utilização de um equipamento institucional ou a adequação do equipamento do colaborador para que sua utilização seja permitida.

11.3. Requisitos mínimos aceitáveis incluem:

Versão de sistema operacional suportado pelo fabricante e com as últimas atualizações devidamente instaladas;

Software antivírus instalado e atualizado;

Programas devidamente licenciados (poderá ser solicitada a exibição da licença ou nota fiscal dos aplicativos para comprovação);

Utilização de usuário e senha para autenticação no sistema operacional;

Utilização de senha de BIOS para inicialização do equipamento (opcional);

Utilização de programa para criptografia de disco (opcional);

11.4. Se for decidido por adequar o equipamento às regras do TJBA, somente após as devidas correções serem realizadas é que seu uso será permitido.

11.5. Em equipamentos particulares, os dados pessoais deverão ficar armazenados em diretório distinto das informações institucionais. Por se tratarem de informações do TJBA, o colaborador que utilizar seu próprio equipamento concorda que a DIN poderá procurar, modificar, remover e controlar o acesso a informações institucionais no equipamento e inclusive realizar análise forense, caso seja necessário.

11.6. Nestes equipamentos, a DIN poderá prestar suporte às ferramentas utilizadas para fins institucionais, como sistemas internos. Para hardware e outros aplicativos (sistema operacional, navegadores, editores de texto e planilha, etc.) a DIN não se responsabiliza pela manutenção e suporte, ficando a cargo do próprio colaborador buscar o suporte do fabricante do equipamento ou aplicativo.

XII - Das regras para instalação e movimentação de ativos

12. Todas as regras para instalação de hardware e software, manutenção e movimentação de equipamentos de informática estão definidas no DECRETO JUDICIÁRIO Nº 922, DE 6 DE OUTUBRO DE 2016, que disciplina a movimentação de equipamentos de informática e a utilização de software e hardware no âmbito do Poder Judiciário do Estado da Bahia.

XIII - Da monitoração

13. Todos os acessos realizados pelos colaboradores são monitorados, inclusive os acessos realizados através dos equipamentos particulares, e os responsáveis possuem ferramentas para acompanhar periodicamente a utilização desses meios por parte dos seus funcionários.

ANEXO III - Gestão de Ativos

I - Da aquisição

1. As áreas do TJBA não podem efetuar aquisições de recursos de informática interagindo diretamente com os fornecedores.

1.1. Para aquisição de SOFTWARES, a Coordenação de Sistemas (COSIS) deverá ser antes contatada para as devidas providências.

II - Do armazenamento de mídias e licenças

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

III - Das configurações, instalações e mudança de equipamentos

3. Todas as regras para instalação de hardware e software, manutenção e movimentação de equipamentos de informática estão definidas no DECRETO JUDICIÁRIO Nº 922, DE 6 DE OUTUBRO DE 2016, que disciplina a movimentação de equipamentos de informática e a utilização de software e hardware no âmbito do Poder Judiciário do Estado da Bahia.

IV - Da instalação de softwares

4. Somente a DIN está autorizada a efetuar instalações de softwares nas estações de trabalho. Somente colaboradores pertencentes ao escopo da DIN podem ter privilégio de administração nas estações de trabalho.

4.1. No ambiente de servidores (equipamentos de TI), apenas a Coordenação de Suporte Técnico (COTEC) tem autorização para realizar a instalação de softwares ou possuir privilégios de administração.

V- Do inventário de informática

5. A DIN, como gestora de todos os recursos de informática do TJBA é responsável por inventariar e manter o controle sobre todos os ativos de informática da instituição.

5.1. Para que o controle se mantenha efetivo, devem ser utilizadas ferramentas automatizadas de coleta de dados dos equipamentos. Esses dados são armazenados em sistema e há um responsável associado a cada ativo da instituição.

5.2. Poderá ser realizado, por amostragem, um inventário físico ao ano para que a acurácia do controle seja validada.

VI- Do descarte de ativos físicos

6. O procedimento para descarte de equipamentos, seja estação de trabalho, equipamento móvel, servidor ou mídias, deve ser realizado de acordo com a Norma de Gestão da Operação de TI.

VII-Dos aplicativos

7. O desenvolvimento de aplicativos é de competência exclusiva da SETIM.

7.1. A política da instituição define que se deve utilizar, sempre que possível, sistemas corporativos, visando garantir a segurança e integridade das informações e do sistema, assim como da documentação, sustentação, integração e compatibilidade com o ambiente tecnológico existente.

7.2. Caso exista a necessidade de desenvolvimento de novos aplicativos, a SETIM deverá ser obrigatoriamente informada para que, em parceria com as áreas de negócio envolvidas, seja elaborado o Estudo de Viabilidade.

7.3. Todo software deve possuir uma “licença de uso” ou um “certificado de autenticidade”.

7.3.1. Todo software caracterizado como “Software Livre” não necessita de licença de uso, mas deverá seguir os procedimentos descritos nesta norma.

7.4. O software de computador, como propriedade intelectual, é protegido pela Lei do Software (Lei 9.609 de 19/02/1998) e pela Lei do Direito Autoral (Lei 9.610 de 19/02/1998). Portanto, qualquer cópia não autorizada constitui crime, violação ao direito autoral e crime de sonegação fiscal.

VIII- Das penalidades

8. De acordo com a Lei do Software e do Direito Autoral, os agentes envolvidos na reprodução ilegal de softwares ficam sujeitas ao pagamento das respectivas indenizações ou perdas e danos em valor correspondente a até três mil vezes o valor de cada cópia do software original, além de sanções penais como multas e detenção.

ANEXO IV - Norma de Classificação da Informação

I - Das disposições gerais

1. Esta norma tem por objetivo definir a classificação das informações da instituição, auxiliando o direcionamento de recursos para proteção das informações e assim evitar vazamentos de informações classificadas (seja em meio físico e/ou digital), prevenindo perdas para a instituição e a quebra de sua confidencialidade, integridade e disponibilidade.

1.1. O acesso as informações com classificação diversa da classificação pública, com qualquer grau de sigilo, por pessoa legalmente autorizada, externa ao quadro de colaboradores, requer assinatura prévia do Termo de Compromisso de Manutenção de Sigilo (TCMS - Anexo I), que evidencie:

I a classificação das informações a serem acessadas;

II a responsabilidade pela manutenção do sigilo;

III a necessidade de aplicação de controles específicos que garantam o acesso somente a pessoas autorizadas.

1.1.1. O acesso à informação classificada em qualquer grau de sigilo, que não o público, também poderá ser permitido, excepcionalmente, a pessoa não autorizada por legislação, mediante assinatura do Termo de Compromisso de Manutenção de Sigilo (TCMS) pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

1.2. Cabe ao TJBA controlar o acesso e a divulgação de informações não públicas por ele produzidas ou custodiadas, assegurando a sua proteção.

1.3. A entidade pública ou privada que, em razão de qualquer vínculo com o TJBA, executar atividades que envolvam o tratamento de informações não públicas, deverá adotar as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança da informação resultante da aplicação desta Norma.

1.4. Caso o acesso à informação não pública seja feito em decorrência de contrato ou convênio, o contrato ou convênio deverá trazer em seus termos expressa previsão de cláusula de confidencialidade e responsabilidade. Nessa hipótese, os empregados, prepostos ou representantes dessas entidades deverão, ainda, previamente ao manuseio das informações sensíveis, firmar o competente TCMS.

II - Dos níveis de classificação

2. As informações produzidas pelo TJBA classificam-se nos graus de confidencialidade público, reservado ou restrito, secreto, pessoal e sigiloso, sendo utilizados os seguintes critérios para cada nível de classificação:

Sigiloso	Informação enquadrada nas hipóteses de sigilo previstas em legislação específica, tal como a de natureza fiscal, bancária, a relacionada a operações e serviços no mercado de capitais, a protegida por sigilo comercial, profissional, industrial ou por segredo de justiça e aquela relativa a denúncias.
Pessoal	Informação que diz respeito à intimidade, vida privada, honra e imagem da pessoa, bem como às liberdades e garantias individuais, na forma do art. 31 da Lei nº 12.527 (LAI), de 18 de novembro de 2011.
Secreto	Informação cuja divulgação tenha impacto significativo nas operações ou objetivos táticos e/ou estratégicos do TJBA, podendo seu acesso ser franqueado, apenas, a determinadas pessoas, a critério do gestor da informação.
Restrito	Informação cuja divulgação cause constrangimento a pessoas ou inconveniência operacional, podendo seu acesso ser franqueado a grupos restritos, como determinadas unidades dentro do órgão, desde que autorizado pelo gestor da informação.
Público	Informação assim considerada por força de lei, ou cuja divulgação não cause qualquer dano, podendo seu acesso ser franqueado a qualquer pessoa.

III - Dos prazos de retenção

3. Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no artigo anterior, terão vigência a partir da data de sua produção, conforme o que segue:

I restrita: 5 (cinco) anos;

II secreta: 15 (quinze) anos;

III pessoal: 100 (cem) anos;

3.1. A restrição de acesso à informação classificada como sigilosa obedece ao prazo estabelecido na legislação específica instituidora do sigilo.

3.2. Alternativamente aos prazos previstos nos incisos I e II do caput, pode ser estabelecido termo final associado à ocorrência de determinado evento, desde que ocorra antes do transcurso do prazo máximo de restrição de acesso. Transcorrido o prazo de restrição de acesso ou consumado o evento que defina o seu termo final, a informação passa, automaticamente, ao grau de confidencialidade público.

3.3. Para a classificação da informação nos graus de confidencialidade previstos no caput, deve ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I o prazo máximo de restrição de acesso ou o evento que defina seu termo final; e

II a gravidade do risco ou dano ao órgão ou ao indivíduo.

IV - Dos papéis e responsabilidades

4. É responsabilidade do gestor da informação definir a classificação dos diferentes tipos de informação manipuladas pelo TJBA. A responsabilidade por classificar e rotular cada informação, documento físico e ativo de informação quanto à sua confidencialidade é da responsabilidade de cada colaborador do TJBA, que deverá obedecer às regras definidas pelo gestor da informação

4.1. Em função do grau de confidencialidade exigido, a classificação da informação de grau “Secreto” é de competência do Presidente do TJBA e dos demais membros da Mesa
Diretora do TJBA e para informações de grau “Restrito”, a competência é do dos membros da Mesa Diretora do TJBA, dos Secretários e dos Dirigentes das Unidades.

V - Do procedimento de classificação das informações

5. A classificação da informação em qualquer grau de sigilo que não o público, deverá ser formalizada no competente Termo de Classificação de Informação (TCI - Anexo II), contendo, no mínimo, os seguintes elementos:

I grau de confidencialidade (ou sigilo) da informação;

II grupo de pessoas que podem acessar a informação;

III assunto sobre o qual versa a informação;

IV fundamento da classificação;

V indicação do tempo de restrição de acesso à informação, contado em anos, meses ou dias, ou do evento que defina o termo final, conforme limites previstos no ITEM III;

VI identificação do gestor da informação, responsável pela classificação; e

VII data da classificação.

5.1. Caso a informação não tenha sido classificada previamente, a classificação deverá ocorrer no momento de sua produção ou recebimento, observados os mesmos requisitos definidos anteriormente, no item 5. No respectivo TCI, deve ser mantido histórico nos casos em que houver redução ou prorrogação de prazo de restrição de acesso ou, ainda, no caso de reclassificação da informação.

VI - Da rotulagem da informação classificada

6. Toda informação deve ser rotulada no momento em que for produzida ou recebida de fonte interna ou externa, seguindo o processo definido no item 5. No momento da produção/recebimento da informação, para fins de aplicação de controles de acesso administrativo e tecnológico à informação classificada, é obrigatória, além do TCI, caso este ainda não exista, a aposição de rótulo que contenha os seguintes elementos:

I grau de confidencialidade;

II grupo de pessoas que pode acessar a informação;

III termo final de restrição de acesso e, quando for o caso, evento que defina o termo final alternativo.

6.1. Para informações de grau público, a rotulagem é facultativa.

6.2. Nos casos em que a aposição de rótulo for inviável, podem ser usadas outras formas de identificar a classificação da informação, desde que os controles existentes sejam suficientes para proteger a informação de forma compatível com sua classificação.

6.3. Quando o sistema de classificação da informação do órgão ou entidade de origem não for equivalente ao do Tribunal, nos termos desta norma, o gestor da informação deverá enquadrá-la em grau de confidencialidade compatível com aquele atribuído na origem.

6.4. Na hipótese de documento que contenha informações classificadas em diferentes graus de confidencialidade, deve ser atribuído ao documento tratamento do grau mais elevado, ficando assegurado o acesso às partes permitidas por meio de certidão, extrato ou cópia, ou, ainda, através de mecanismos eletrônicos, com ocultação das partes não permitidas.

VII - Da transferência de informações

7. O envio de informações que não sejam públicas para outras instituições, deve ser feito de forma segura, protegendo os arquivos com senha e enviando a senha por outro meio que não seja o mesmo por onde a informação principal tenha sido transmitida. Ex.: Ao enviar um arquivo com a classificação “Secreta” por e-mail, a senha deve ser repassada por telefone ou comunicador instantâneo.

7.1. Quando houver necessidade de fornecimento de informações de classificação “Restrito”, “Secreto”, “Pessoal” ou “Sigiloso” para instituições terceiras (público ou privadas), é obrigatório a assinatura TCMS pela parte que receberá essa informação, inclusive com relação à proteção de dados de terceiros, quando o caso.

VIII - Da reclassificação e reavaliação da classificação da informação

8. As informações produzidas pelo TJBA podem ser reclassificadas por iniciativa própria do gestor da informação ou mediante provocação, cabendo comunicação imediata da alteração aos custodiantes da informação para correta rotulação. Qualquer interessado pode provocar o gestor da informação com vistas à reclassificação. A decisão acerca do pedido de reclassificação da informação deverá ser devidamente fundamentada.

8.1. A classificação das informações no grau de confidencialidade secreto deve ser periodicamente reavaliada pelo gestor da informação, mediante provocação ou de ofício, para reclassificação ou redução do prazo de restrição de acesso. Para isso, deve ser observado:

I o prazo máximo de restrição de acesso à informação previsto no Item III deste documento;

II o prazo máximo de quatro anos para realização de cada revisão de ofício;

III a permanência das razões da classificação; e

IV a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação.

8.2. Na hipótese de redução do prazo de restrição de acesso, o novo prazo deve manter como termo inicial a data da produção da informação.

IX - Das informações pessoais

9. O tratamento das informações classificadas no grau de confidencialidade pessoal deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

9.1. As informações a que se refere este item, relativas à intimidade, vida privada, honra e imagem:

I têm o seu acesso restrito a agentes públicos legalmente autorizados e à pessoa a que elas se refiram; e

II podem ter autorizada sua divulgação ou acesso por terceiros mediante previsão legal ou consentimento expresso da pessoa a que elas se refiram.

9.2. Caso o titular das informações pessoais esteja morto ou ausente, os direitos de que trata este artigo assistem ao cônjuge ou companheiro, aos descendentes ou ascendentes, conforme o disposto no parágrafo único do art. 20 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), e na Lei nº 9.278, de 10 de maio de 1996.

9.3. O consentimento referido não é exigido quando as informações forem necessárias:

I à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se refiram;

III ao cumprimento de ordem judicial;

IV à defesa de direitos humanos; ou

V à proteção do interesse público e geral preponderante.

9.4. A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não pode ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

9.5. Compete à Corregedoria do TJBA atender às solicitações de informações pessoais solicitadas.

X - Do descarte das informações

10. O TJBA deve descartar suas informações quando os prazos definidos no Item III expirarem. As informações que não forem públicas devem ser descartadas de maneira segura, de forma que não seja possível recuperá-las. Informações em meio físico (papel) devem ser descartadas após serem fragmentadas.

10.1. As informações em meio digital devem ser removidas de maneira segura e os ativos de armazenamento dessas informações devem ser descartados de acordo com o que consta nas normas de Gestão de Ativos e de Gestão da Operação de T.I.

XI - Das disposições finais e transitórias

11.1. A cada grau de confidencialidade, definido nos termos desta Norma, corresponde um conjunto específico de controles administrativos e tecnológicos compatíveis com os danos potenciais às operações vitais ao negócio do TJBA ou à imagem, tanto do TJBA quanto do indivíduo, decorrentes do uso ou do acesso não autorizado à informação.

11.2. Em caso de dúvida na identificação do gestor da informação, compete ao Comitê Gestor de Segurança da Informação defini-lo.

11.3. O TJBA deverá proceder à reavaliação das informações por ele produzidas anteriormente à data de vigência desta Norma, com vistas à sua classificação ou reclassificação.

11.4. A Diretoria de Informática (DIN) procederá aos ajustes necessários nas soluções de TI decorrentes do disposto nesta Norma.

ANEXO IV.1

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

Eu, [Qualificação: nome, nacionalidade, CPF, identidade (no, data e local de expedição), filiação e endereço], perante o Tribunal de Justiça do Estado da Bahia (TJBA), DECLARO ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, comprometendo-me a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo TJBA e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo:

(i) informações classificadas em qualquer grau de sigilo;

(ii) informações relativas aos materiais de acesso restrito do TJBA, salvo autorização da autoridade competente.

Declaro que [recebi] [tive acesso] ao (à) [documento ou material entregue ou exibido ao signatário], e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

___[Local e data]___

ANEXO IV.2

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

ÓRGÃO/ENTIDADE:

CÓDIGO DE INDEXAÇÃO:

GRAU DE SIGILO:

CATEGORIA:

TIPO DE DOCUMENTO:

DATA DE PRODUÇÃO:

FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO:

RAZÕES PARA A CLASSIFICAÇÃO:

(idêntico ao grau de sigilo do documento)

PRAZO DA RESTRIÇÃO DE ACESSO:

DATA DE CLASSIFICAÇÃO:

AUTORIDADE CLASSIFICADORA

Nome:

Cargo:

AUTORIDADE RATIFICADORA

(quando aplicável)

Nome:

Cargo:

DESCLASSIFICAÇÃO em ____/____/_____

(quando aplicável)

Nome:

Cargo:

RECLASSIFICAÇÃO em ____/____/_____

(quando aplicável)

Nome:

Cargo:

REDUÇÃO DE PRAZO em ____/____/_____

(quando aplicável)

Nome:

Cargo:

PRORROGAÇÃO DE PRAZO em ___/ ____/_____

(quando aplicável)

Nome:

Cargo:

_____

ASSINATURA DA AUTORIDADE CLASSIFICADORA

_____

ASSINATURA DA AUTORIDADE RATIFICADORA (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO (quando aplicável)

ANEXO V – Norma de Gerenciamento de Acessos

I - Das disposições gerais

1. Os sistemas de informação são ativos importantes para a instituição. Todos seus colaboradores 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.

1.2. A gestão das práticas de segurança da informação é de responsabilidade da Secretaria da Tecnologia da Informação e Modernização (SETIM), que direcionará todas as questões relacionadas a este tópico.

1.3. 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).

II - Da definição de responsabilidades

2. A concessão de acessos aos sistemas em utilização no TJBA é de competência da área gestora.

III - Da gestão dos acessos (concessão, transferência e exclusão)

3. É de responsabilidade do departamento requisitante, solicitar ao responsável pelo processo de negócio a inclusão ou alteração dos perfis de acesso do mesmo. Para decidir sobre a aprovação ou não das solicitações, o responsável pelo processo de negócio deverá avaliar a solicitação com base nas responsabilidades e atividades desempenhadas pelo colaborador.

3.1. Todos os colaboradores deverão utilizar, obrigatoriamente, o mesmo processo de concessão de acesso para obter uma conta de acesso aos sistemas de informação.

3.2. Qualquer solicitação de acesso, deverá ser feita através de chamado.

3.3. Após realizado o processo, o administrador do ambiente informará a inclusão/exclusão dos acessos ao solicitante (usuário).

3.4. As contas de acesso pertencentes a prestadores de serviços e visitantes deverão ser configuradas para expirar e serem bloqueadas automaticamente pelos sistemas de informação ao término de seus projetos ou período de prestação de serviço, sendo que essa data deverá ser definida pela área solicitante. O tempo máximo para configurar a expiração de um acesso de prestador de serviços é de 1 (hum) ano. Na necessidade de se prorrogar esse acesso, todo o fluxo deve ser repetido.

3.5. Caso o terceiro pare de prestar serviços para o TJBA antes do período previsto, é dever do fiscal do contrato comunicar a Central de Serviços, via abertura de chamado, que determinado terceiro já não presta mais serviços para o TJBA e, portanto, já não necessita mais dos acessos.

3.5.1. Enquanto a área responsável não notificar o desligamento do terceiro ou prestador de serviço, o acesso será mantido e as responsabilidades atribuídas para o usuário em questão, permanecerão com a área solicitante.

3.6. Cabe a área responsável comunicar através de chamado na Central de Serviço, para evidenciar a referida comunicação em tempo hábil, sobre os desligamentos de colaboradores ocorridos para que a Central de Serviço efetue as devidas exclusões dos acessos à rede/sistemas acessados pelo ex-colaborador.

3.7. É de responsabilidade da área responsável notificar através de chamado no Central de Serviço que determinado colaborador foi transferido de uma área para outra.

3.8. Após notificação da transferência, a DIN deverá entrar em contato com o funcionário transferido e solicitar um novo chamado para que sejam configurados os novos acessos. A partir dessa data, o colaborador terá 7 (sete) dias para abrir o chamado.

3.9. Caso o chamado de solicitação dos novos acessos não seja enviado no prazo de 7 (sete) dias, a DIN poderá bloquear todos os acessos vigentes do funcionário em questão até a regularização dos mesmos na nova área.

3.9.1. Nos casos onde o funcionário é transferido sem a ciência do Departamento de Recursos Humanos, a transferência não será reconhecida pela DIN. Sendo assim, as alterações eventualmente solicitadas, não serão atendidas ou efetivadas.

IV - Da aprovação

4. As solicitações de criação de usuários e alterações de perfis de acesso deverão passar, obrigatoriamente, por 2 (dois) níveis de análise e aprovação formais, sendo 1 (um) nível de aprovação e 1 (um) nível de revisão independente. Dessa forma, as aprovações deverão seguir um fluxo específico contemplando os seguintes passos:

Análise e aprovação do superior do próprio colaborador solicitante;

Análise e aprovação do responsável pelo processo de negócio ao qual está sendo solicitado acesso;

4.1. A “Lista dos Aprovadores dos Sistemas” está disponível para consulta na Intranet do TJBA.

4.2. Caso o responsável pelo funcionário e o responsável do processo de negócio em questão sejam a mesma pessoa, será necessária apenas uma aprovação para a liberação desse acesso.

4.3. Sem a devida solicitação e aprovação dos responsáveis, o funcionário permanecerá sem o acesso solicitado.

4.4. Não são permitidos casos onde o responsável (coordenadores, gerentes e etc.) aprove seu próprio acesso. Nestes casos, seu superior imediato deve aprovar a solicitação.

V - Da retirada parcial de acessos

5. A retirada parcial dos acessos poderá ocorrer sempre que um funcionário tiver suas atividades diárias alteradas ou então quando determinada responsabilidade ou módulo de acesso não for mais necessário para seu trabalho.

5.1. O processo de exclusão parcial dos acessos deverá ser aprovado pelo responsável pelo funcionário. Após realizado o processo, o administrador do ambiente, confirmará a exclusão parcial dos acessos ao solicitante (usuário).

VI - Do bloqueio de acessos

6. O bloqueio dos acessos à rede (login no Windows) dos Colaboradores em férias se dará automaticamente após sincronia entre o servidor de rede e o sistema de Recursos Humanos.

6.1. Nos casos de licença maternidade ou de afastamentos por mais de 15 (quinze) dias, a Central de Serviço deverá ser comunicada através de chamado para evidenciar a referida comunicação, para que sejam efetuados os bloqueios dos acessos à rede/sistemas de acesso pelo Colaborador.

VII - Das regras gerais de acesso

7. Não será permitido, em hipótese alguma, o compartilhamento das contas de acesso entre os usuários dos sistemas de informação. Quaisquer exceções deverão ser verificadas pela Área de Segurança da Informação

7.1. 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 responsável único, salvo após aprovação da área de Segurança da Informação, que providenciará a aprovação para criação desta conta.

7.2. Todas as contas de acesso devem possuir um único responsável (funcionário, prestador de serviço ou visitante), com indicação de seu nome completo (nome e sobrenome). No caso de visitantes e prestadores de serviço, a conta de acesso deverá ser criada com indicação da empresa que o prestador de serviço trabalha, além do nome completo (nome, sobrenome e CPF).

7.3. Não é permitida a existência de usuários duplicados nos ambientes de produção dos sistemas de informação, ou seja, um funcionário com acesso a 2 (duas) ou mais contas de acesso ativas, que podem ter nomes iguais, semelhantes ou diferentes.

7.4. Não é permitida a utilização de usuários de sistema / serviço para realização de tarefas administrativas por parte dos analistas responsáveis pela administração dos sistemas de informação nem por parte dos administradores dos servidores que abrigam os sistemas de informação.

7.5. Os funcionários da DIN poderão ter acessos do tipo “Administrador” e acessos operacionais para efetuarem atividades do dia a dia. Esses colaboradores deverão possuir dois usuários distintos, um com privilégios de “Administrador” e outro usuário sem privilégios especiais. Os usuários com privilégios de “Administrador” não devem possuir acesso à internet, diretórios de arquivos ou a sistemas que utilizem o Active Directory para autenticação. Somente o usuário comum (sem privilégios especiais) poderão ter esses acessos.

7.6. Não são permitidas contas de usuários prestadores de serviço ou de visitantes com direitos de administração nos ambientes de produção de qualquer sistema de informação, a menos que sejam prestadores de serviços da DIN e que sejam devidamente autorizados pelo responsável da área.

7.7. Apenas em ambientes de homologação, desenvolvimento e teste, usuários da DIN e consultores poderão ter acessos administrativos. Quaisquer exceções deverão ser devidamente justificadas e autorizadas pela área de Segurança da Informação.

VIII - Da revisão de acessos

8. A área de Segurança da Informação deverá analisar periodicamente os acessos ativos dos sistemas de informação.

8.1. 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.

8.2. É importante ressaltar que essa revisão não leva em conta os perfis de acesso de cada usuário, levando em conta apenas os acessos ativos.

8.3. Tal revisão será realizada ao menos 1 (uma) vez por ano, para cada sistema definido, de acordo com calendário estabelecido pela Área de Segurança da Informação.

8.4. Ao fim de cada revisão, um relatório será criado pelas áreas de Segurança da Informação e será enviado para as áreas responsáveis pela concessão de acesso aos sistemas.

8.5. Se durante o trabalho de revisão forem encontrados acessos indevidos, os mesmos poderão ser bloqueados imediatamente, sendo liberados após regularização, se for o caso.

IX - Da revisão dos perfis de acesso

9. Os perfis de acesso aos sistemas de informação do TJBA devem estar condizentes com as atribuições de cada usuário, respeitando as melhores práticas de segregação de função, evitando assim, conflitos de interesses. Essa medida visa proteger os registros dos usuários nos sistemas utilizados pela instituição, garantindo que apenas pessoas autorizadas possam acessar e alterar as informações.

9.1. A revisão dos perfis deve ser realizada anualmente, sendo o responsável por essa atividade o gestor aprovador de cada sistema/módulo.

9.2. A Lista dos Aprovadores dos Sistemas, com o nome dos gestores aprovadores de cada sistema, está disponível para consulta na Intranet do TJBA

9.3. A área de Segurança da Informação será responsável por contatar os aprovadores, definir em conjunto com os mesmos o cronograma da atividade, enviar a lista de usuários ativos e seus respectivos perfis de acesso e providenciar as adequações indicadas pelo aprovador.

9.4. Caso em alguma das revisões seja necessária alguma modificação nos perfis/acessos, a área de Segurança da Informação será responsável por providenciar o chamado para que a alteração solicitada seja realizada.

X - Do gerenciamento de privilégios administrativos

10.0 Complementando os itens anteriores, as contas de acesso privilegiado a sistemas corporativos, equipamentos de redes e sistemas operacionais, devem ser restritas aos funcionários da DIN que não consigam desempenhar suas funções diante do negócio sem que tal tipo de acesso seja concedido.

10.0.1. Os acessos privilegiados devem ser solicitados seguindo o mesmo processo já definido nesta norma.

X.1 - Do acesso em banco de dados

110.1.1 O acesso direto a banco de dados em ambientes produtivos, por parte de colaboradores que não fazem parte da DIN não é permitido, tanto para consulta quanto para edição de dados. Eventuais exceções deverão ser formalizadas e aprovadas pelo responsável da área solicitante e pelo gestor da DIN.

ANEXO VI - Norma de Gestão de Operação de TI

I - Da configuração de equipamentos

1. Para todos os servidores, independentemente do sistema operacional utilizado, a DIN é responsável por realizar toda a configuração lógica dos equipamentos, desde sua primeira inicialização até sua desativação.

1.2. No momento que um novo equipamento é disponibilizado para a equipe da DIN, deve ser aplicado o respectivo roteiro de configuração, para que as regras mínimas de segurança exigidas para o equipamento sejam implementadas, como por exemplo, atualização de sistema operacional, atualizações de firmware, alteração de senha padrão, alteração do nome do usuário administrador, etc. As regras do roteiro de configuração estão disponíveis na Base de Conhecimento.

1.3. Para os equipamentos utilizados pelos colaboradores (notebooks, desktops, smartphones, etc.), a responsabilidade por realizar a configuração inicial é da DIN, que receberá os equipamentos, fará toda a configuração necessária, aplicando o roteiro de configuração do respectivo equipamento, instalando os softwares e aplicativos necessários para a utilização do colaborador e realizará a entrega do equipamento para o colaborador que ficará responsável pelo uso do equipamento, orientando-o sobre as responsabilidades aplicáveis e lavrando o respectivo Termo de Entrega.

1.4. Todos os equipamentos devem ser sincronizados com servidor NTP (seja interno ou externo). A sincronia é importante para que todos os ativos estejam com o mesmo horário configurado, evitando assim, divergência de informações entre os ativos.

II - Do backup de informações

Seção I - Da geração

2. As especificações (Full ou incremental, por exemplo), bem como 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. Após sua definição por parte da área responsável pela informação ou ativo de informação (sistema ou serviço), é necessário que seja preenchido o formulário de solicitação de backup disponível na Base de Conhecimento. As mídias de backup devem ser armazenadas em local distante do datacenter principal que ofereça proteções contra alta temperatura, umidade e acessos não autorizados.

Seção II - Do manuseio e transporte das mídias de backup

2.1. 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.

2.2. Toda e qualquer movimentação de mídias entre sites deve ser documentada, através de controle próprio detalhando dia, hora e responsável pela movimentação.

Seção III - Do armazenamento das mídias de backup

2.3. 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;

2.4. As mídias de armazenamento utilizadas para rotinas de backup devem ser adequadas aos equipamentos utilizados para realização de backup.

2.5. A DIN 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.

2.6. 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.

Seção IV - Dos testes

2.7. Semestralmente a equipe da DIN deverá realizar testes de Recuperação de Dados por amostragem, com o objetivo de atestar a integridade e disponibilidade dos dados armazenados.

2.8. A recuperação deve ser integral de pelo menos um servidor/sistema escolhido aleatoriamente e deve ser planejada e documentada para fins de auditorias futuras.

Seção V - Do registro de falhas

2.9. As falhas referentes a problemas com o processo de backup e restore de informações devem ser registradas e reportadas.

2.10. 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.

Seção VI - Do restore dos dados

2.11. A restauração das cópias de backup deve ser realizada através da abertura de chamado com a aprovação do proprietário da informação.

2.12. Para casos relacionados a incidentes com servidores, fica a critério da DIN avaliar a necessidade de recuperação, a fim de restabelecer o ambiente o mais rápido possível.

Seção VII - Dos outros backups

2.13. Para os equipamentos que não possuem integração nativa com a ferramenta de backup e que necessitem de backup de suas configurações (ex.: switches, firewall, etc.), é necessária a intervenção da equipe da DIN para que ao menos mensalmente seja realizada uma cópia do arquivo de configuração do equipamento e esse arquivo deve ser armazenado em local seguro.

2.14. Esse processo deve ser o mais automatizado possível, para que, em caso de necessidade, seja possível restaurar a configuração de um equipamento da maneira mais rápida possível, sem que haja a necessidade de realizar toda a reconfiguração do equipamento, partindo da configuração original do fabricante.

2.15. A cópia desses arquivos de configuração deve ser armazenada no servidor de arquivos do TJBA, com acesso restrito aos administradores, para que eles sejam copiados para as mídias de backup.

Seção VIII - Da substituição e descarte de mídias

2.16. Todas as mídias fixas ou removíveis devem possuir descartes seguros.

2.17. 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.

2.18. 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.

2.19. As mídias devem ser destruídas adequadamente antes de serem descartadas, de forma que os dados não possam ser recuperados, a fim de evitar o vazamento de informações confidencias e críticas para o negócio.

2.20. Todas as mídias descartadas devem ser registradas, de forma a manter uma trilha de auditoria.

III - Da manutenção de equipamentos

3. A responsabilidade pela manutenção dos equipamentos é da DIN.

3.1. Em caso de necessidade de suporte ou alteração (física ou lógica), cada área deverá realizar os procedimentos necessários para que a operação retorne ao normal o mais rápido possível, de acordo com o impacto e a urgência demandada.

3.2. Em caso da necessidade de contatar empresas terceiras para a realização de consertos e reparos, cada área será responsável por fazer esse contato e acompanhá-lo durante toda a manutenção, atestando que, ao fim do processo de reparo, a operação seja normalizada.

VI - Da atualização de equipamentos

4. Devido às diferentes metodologias utilizadas pelos fabricantes na disponibilização de atualizações para seus produtos, e pelo impacto que pode ser gerado durante uma atualização, é necessário classificar os ativos em grupos, para que sejam tratados adequadamente.

4.1. Deverá ser criada pela DIN um documento com a classificação dos ativos.

Seção I - Do cronograma de liberação de atualizações

4.2. As atividades de atualização devem seguir o calendário de atualizações, de acordo com a classificação dos ativos. Para qualquer mudança eu venha a ocorrer, as atividades de atualização devem seguir o processo de Requisição de Mudanças e ser realizada somente após os devidos testes e aprovações.

Seção II - Das atualizações críticas e emergenciais

4.3. No caso do lançamento de patches críticos por parte dos fabricantes, que podem ocorrer em qualquer data, até mesmo fora da janela reservada para atualização, a área de TI deve fazer uma avaliação da vulnerabilidade que o patch crítico corrige e caso seja constatado que o risco é alto, deverá ser montada uma Requisição de Mudança Emergencial, para aplicação da correção o mais rápido possível, afim de mitigar o risco de exposição da empresa.

Seção III - Dos ativos de rede e ativos de infraestrutura

4.4. Devido à complexidade em realizar a atualização em ativos de rede e infraestrutura, a atualização desses equipamentos ocorrerá em intervalos regulares.

4.4.1. Toda atualização desses ativos deverá ser devidamente testada e implementada através de Requisição de Mudança.

Seção IV - Exceções

4.5. Caso seja detectado que uma ou mais atualizações estejam impactando negativamente o ambiente ou os testes não tenham obtido sucesso, essa atualização deverá ser registrada como “não aplicável” no ambiente do TJBA e a área de Segurança da Informação deverá sugerir, se for possível tecnicamente, formas de mitigar o risco de exploração dessa vulnerabilidade e monitorar por possíveis ameaças que possam explorá-la.

4.6. Como forma de reduzir o risco de exploração de vulnerabilidades devido a falta de atualização dos servidores e estações de trabalho, uma solução de Virtual Patch deve ser instalada nos ativos. Essa solução não deve ser utilizada como única forma de proteção e sim como uma camada adicional de proteção.

V - Do gerenciamento de logs

5. Todos os sistemas operacionais, sistemas de aplicativos e equipamentos de redes devem ser devidamente configurados para que gerem logs de eventos, segurança e auditoria.

5.1. 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.

5.2. Os seguintes itens devem ser configurados para gerarem logs em todos os equipamentos e serão configurados quando houver a possibilidade técnica:

Inicialização e desligamento do sistema (S.O.);

Tentativas de acesso (login) e de saída do sistema (logoff);

Tentativas não autorizadas de acesso aos arquivos de sistema;

Mensagens do sistema operacional;

Manutenção e mudanças na configuração do sistema;

Logs de Auditoria;

Log do Servidor Web.

5.3. A equipe de Segurança da Informação é responsável por determinar quais os eventos que devem ser logados por cada tipo de ativo.

5.4. O servidor de repositório dos logs deve ter acesso restrito somente à área de Segurança da Informação do TJBA. Tanto o acesso ao sistema operacional quanto à ferramenta de gestão dos logs deve ter o acesso controlado.

5.5. O servidor de repositório deve ter seus dados copiados para fitas de backup periodicamente, com tempo de retenção de 5 (cinco) anos, para que os dados possam ser recuperados em caso de necessidade futura.

VI - Da gestão de vulnerabilidades

6. A área de Segurança da Informação deve realizar a análise (também chamado de scan) de vulnerabilidade mensalmente através do uso de ferramentas apropriadas e de conhecimento de um técnico especialista para a função. O resultado do scan de vulnerabilidade deve ser analisado criticamente pela equipe de Segurança da Informação e os itens identificados como críticos, as medidas de correção devem ser planejadas e implementadas, seguindo todo o processo de Gestão de Mudança definido pelo TJBA.

6.1. Nos casos onde não seja possível implementar a correção da vulnerabilidade identificada, alternativas devem ser analisadas entre as áreas de Segurança da Informação, DIN e área de negócio responsável pelo ativo, caso seja aplicável. Em conjunto, as áreas deverão encontrar uma solução para mitigar a vulnerabilidade identificada ou, em último caso, aceitar o risco pois a implementação de medidas mitigatórias pode não ser viável.

6.2. Nos casos onde o risco seja aceito, deve ser feita uma documentação formalizando que a vulnerabilidade existe, que é de conhecimento dos responsáveis pela SETIM e pela área de negócio envolvida com o ativo e que todos os envolvidos aceitam o risco, pois ele é inerente ao negócio.

6.3. Semestralmente, a área de Segurança da Informação deve gerar indicadores com a quantidade de vulnerabilidades identificadas, resolvidas, pendentes e aceitas. Esses indicadores deverão ser divulgados para o Comitê Gestor de Segurança da Informação.

VII - Da gestão de capacidade

7. A DIN será responsável por monitorar os sistemas/equipamentos, verificando se o planejamento de capacidade atende aos requisitos do negócio a fim de não causar degradação dos sistemas e por consequência disso, lentidão nas operações ligadas ao negócio da empresa.

7.1. Para isso, deverá ser estabelecido um processo para gestão de capacidade, onde serão utilizados sistemas de monitoria de ativos que façam a medição dos recursos como utilização de processamento, utilização de memória, capacidade de armazenamento em disco/storage, entre outros.

7.2. O acompanhamento dos recursos deve ser rotineiro e um relatório semestral deverá ser enviado para a alta direção da instituição, inclusive destacando eventuais insuficiências (gargalos) de recursos que possam ocorrer em um curto período. Com esse relatório, poderão ser decididos os planos de ação para crescimento orgânico/ajuste da capacidade ofertada.

VIII - Da desativação de ativos

8. Quando for identificado que um ativo não é mais necessário, não atende mais as necessidades do TJBA ou estiver danificado e o conserto não seja viável, deve ser iniciado o processo de desativação desse equipamento.

8.1. Todo equipamento deve ter seus dados definitivamente excluídos ou tornado inacessíveis antes de ser descartado. Para servidores e estações de trabalho que estiverem funcionais, seus discos rígidos devem sofrer um processo de “wipe”, ou seja, a remoção completa dos dados.

8.2. Para os equipamentos que não estiverem operacionais, deverá ser feita a destruição física do disco rígido, para que todos os dados não possam ser aproveitados por terceiros.

8.3. Para outros equipamentos como, por exemplo, switches e firewalls, as configurações deverão ser retornadas para o estado padrão de fábrica antes do processo de descarte ser iniciado. Para os casos onde não houver possibilidade de retornar as configurações originais, deverá ser realizada a destruição física dos equipamentos, para que não possam ser reaproveitados.

IX - Do descarte de ativos

9. Após a correta desativação e remoção dos dados de cada ativo que não for mais necessário ao TJBA, o descarte de material deve ser realizado de maneira adequada, através de empresa especializada nesse tipo de atividade, que emita certificado atestando que todos os ativos foram adequadamente descartados, obedecendo à Lei nº 12.305/10, que institui a Política Nacional de Resíduos Sólidos (PNRS).

ANEXO VII – Práticas de Desenvolvimentos Seguros

I - Da segregação de ambientes

1. Com o objetivo de mitigar riscos e evitar danos aos negócios da instituição, faz-se necessário a segregação dos ambientes de desenvolvimento, teste, homologação e produção.

1.1. Os desenvolvedores devem ter acesso apenas aos ambientes de desenvolvimento, teste e homologação, incluindo acesso ao sistema operacional e banco de dados. Nesses ambientes, deverão ser realizados todos os desenvolvimentos e testes dos aplicativos e após a definição da versão final, deverá ser montada a documentação de como essa implementação/melhoria deverá ser aplicada em ambiente de produção.

1.2. A aplicação em ambiente de produção deverá ser requisitada formalmente através de Formulário de Requisição de Mudança e alinhada com o Comitê de Mudança.

1.3. Nos ambientes de produção (sistemas operacionais, banco de dados e etc.), apenas os analistas de infraestrutura poderão ter acesso de administrador.

1.4. Para os sistemas que não possuírem ambientes de desenvolvimento, teste ou homologação, será necessária a aprovação formal por parte dos membros do Comitê Gestor de Segurança da Informação para a liberação de acesso a terceiros e desenvolvedores.

II - Da descaracterização de banco de dados

2. Os bancos de dados dos ambientes de desenvolvimento, teste ou homologação deverão ter os campos que contenham informações de identificação pessoal descaracterizados, ou seja, não deverão conter dados reais de colaboradores e usuários dos serviços prestados pelo TJBA.

III - Das principais práticas de desenvolvimento de software

3. O desenvolvimento de novas soluções deve estar adequado ao nível atual de inovação e tecnologia disponíveis no mercado. Para tanto, ao iniciar o projeto para desenvolvimento de um novo sistema, deverão ser incluídos nos projetos os seguintes temas:

Portabilidade e interoperabilidade;

Ser compatível com dispositivos móveis;

Ser responsivo;

Oferecer documentação para utilização e administração;

Oferecer suporte para assinatura baseado em certificado emitido por Autoridade Certificadora credenciada na forma da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil e ICP Jus);

Atender ao Modelo de Acessibilidade em Governo Eletrônico, institucionalizado pelo Ministério do Planejamento, Orçamento e Gestão.

Atender aos requisitos de segurança, conforme descrito nos próximos itens deste documento.

Seção I - Da validação dos dados de entrada

3.1. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas para a validação dos dados de entrada:

Tratar os campos de entrada de dados aos sistemas, de modo que apenas dados legítimos sejam aceitos, evitando, por exemplo, caracteres como “%”, “!”, “<”,”>”,” ’ ”, “/”, “”, “ . ”, etc.

Criar uma “lista branca” de entradas válidas;

Validar os tipos de dados esperados, bem como seu tamanho e intervalo;

Realizar toda a validação diretamente no servidor, não no cliente;

Definir um conjunto de caracteres comuns para validação (UTF-8, por exemplo).

Seção II - Do gerenciamento de autenticação

3.2. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas para o gerenciamento da autenticação:

Evitar com que os formulários carreguem automaticamente informações de autenticação, como usuários e senhas;

Todos os controles de autenticação devem ser efetuados do lado do servidor, não do cliente;

Campos de troca de senha devem solicitar no mínimo as informações da senha antiga, da senha nova e a confirmação da senha;

Todo o trânsito de credenciais de acesso deve ser criptografado;

Funções de “Esqueci minha senha” não devem revelar a senha cadastrada para o usuário, pois isso implica em gravá-la em texto claro no banco de dados;

Implementar funções que bloqueiem a utilização de senhas fracas e bem conhecidas, como 1234, 123456, abcdef, etc.;

Se a aplicação gerenciar um repositório de credenciais, as senhas não devem estar armazenadas em formato aberto, devendo ser armazenado apenas o “hash”. Para gerar os Hashes das senhas, deve-se utilizar um algoritmo como o SHA1 ou superior;

Não armazenar senhas diretamente no código fonte;

Somente utilizar requisições do tipo “POST” para tratamento de credenciais de autenticação;

Implementar parâmetros de senha fortes configuráveis como por exemplo, tamanho mínimo de senha, quantidade de tentativas antes de bloquear a conta, histórico de senhas, tempo mínimo para troca de senha, tempo máximo para troca de senha, etc.

Seção III - Do gerenciamento de sessões

3.3. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto ao gerenciamento de sessões:

As mensagens de erro de autenticação não devem indicar qual parte da autenticação está errada (se o usuário ou a senha). Elas devem trazer uma mensagem de erro idêntica, independente de qual parte esteja errada;

Utilize os gerenciadores de sessão padrão da linguagem de programação utilizada;

Invalide todas as sessões quando o usuário efetuar logoff do sistema;

O botão de “sair” (logoff) deve estar presente em todas as páginas autenticadas;

Estabelecer um tempo de inatividade, para que uma sessão não fique aberta por tempo indeterminado;

Em ambientes de produção, nunca divulgue o ID da sessão diretamente na URL, em mensagens de erro ou logs.

O sistema deve garantir que, quando um usuário fizer login no sistema, seja gerada uma nova sessão e um novo ID de sessão, sendo esses dados únicos e suficientemente longos e aleatórios, para evitar reuso de sessão e descoberta através de método de tentativa e erro;

Os tokens de sessão devem possuir os atributos “HttpOnly” e “Secure” habilitados;

Implementa controle de sessão, de modo que um usuário não possa ter mais do que uma sessão ativa. Caso uma nova sessão seja aberta, a sessão antiga deve ser invalidada;

Nos casos onde as sessões durem um longo período, revalidar a sessão de tempos em tempos, sendo esse tempo a ser definido internamente;

As aplicações onde for pertinente, podem apresentar faixas de horário de autenticação, não permitindo que usuários autentiquem no sistema fora do horário especificado.

Seção IV - Do controle de acesso

3.4. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto ao controle de acesso:

Quando ocorrer alguma falha no controle de acesso, o sistema deve estar preparado para trabalhar no modo “fail-secure”, ou seja, em caso de falhas, o acesso seja bloqueado;

Restringir o acesso às URLs, funções, referências, serviços e dados somente a usuários autorizados;

Permitir que apenas usuários com os devidos privilégios possam alterar as configurações de segurança;

Possuir perfis de acesso que sejam customizáveis pelos administradores.

Seção V - Das práticas de criptografia

3.5. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto a utilização de criptografia:

Devem ser implementadas funções de criptografia no lado do servidor para proteger os dados sensíveis das aplicações;

A senha mestre e as chaves privadas devem ser protegidas contra acessos não autorizados.

Seção VI - Do tratamento de erros e logs

3.6. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto ao tratamento de erros e logs:

As mensagens de erro exibidas na tela devem ser genéricas e não devem mostrar informações sensíveis sobre a infraestrutura ou lógica da aplicação. Essas informações devem estar disponíveis apenas nos arquivos de logs no servidor;

As páginas de erro devem ser personalizadas;

A aplicação deve ser capaz de realizar o correto gerenciamento de memória;

Apenas pessoal autorizado deve ter acesso aos logs (administradores do ambiente e desenvolvedores);

Identificadores de sessão e senhas não devem ser incluídos em logs e mensagens de erro;

Todas as falhas de validação de entrada de dados devem ser registradas em logs

Todas as tentativas de autenticação devem ser registradas, tendo resultado em sucesso ou não;

As tentativas de conexão com tokens de sessão inválidos ou expirados devem ser registradas em logs;

Todos os registros de eventos que ocorrem nos sistemas devem ser armazenados em arquivos de logs. Periodicamente (recomendado 1 vez ao dia, mas pode variar de acordo com o volume de registros), o arquivo com os logs deve ser “fechado”, ou seja, não receberá mais registros. Um novo arquivo de log deve ser criado. O arquivo anterior deve ter seu nome alterado para facilitar a sua localização e evitar que seja duplicado. O hash desse arquivo deve extraído e armazenado de forma segura e em local distinto arquivo original (como por exemplo, no próprio sistema), para controle de integridade do arquivo de log.

A aplicação deve ser capaz de gerar trilha de auditoria para que haja rastreamento das ações realizadas pelos usuários. A trilha gerada deve ser capaz de registrar tanto informações de login, gerenciamento de acessos (troca de senha, alteração de perfil), logoff, quanto informações de alterações sistêmicas, como por exemplo, o que foi alterado (campo e/ou valor), quando foi alterado (timestamp), quem fez a alteração (login), de onde foi feita a alteração (IP e/ou hostname), qual era o valor anterior (manter todos os registros, não apenas o último antes da alteração) e valor para o qual foi alterado.

Seção VII - Da proteção de dados

3.7. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto a proteção de dados:

Os usuários devem possuir acesso somente ao mínimo de informações possível para a correta execução de suas atividades diárias;

O código fonte da aplicação deve ser protegido de acesso não autorizado;

Todos os comentários devem ser removidos nos ambientes de produção;

Desativar funções de cache em partes da aplicação que contenham informações sensíveis.

Seção VIII - Da segurança nas comunicações

3.8. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto a segurança nas comunicações:

Todo o tráfego de informações sensíveis deve ser realizado através de algoritmos de criptografia seguros (TLS 1.1 ou superior);

Para aplicações acessíveis pela internet, os certificados emitidos devem ser válidos, com nome de domínio correto, dentro do prazo de validade e instalados adequadamente;

Toda informação sensível deve estar protegida por conexão TLS 1.1 ou superior.

Seção IX - Da configuração do sistema

3.9. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto a configuração do sistema:

Gerir adequadamente as versões dos aplicativos instalados nos servidores que fornecem a infraestrutura para a aplicação;

Desativar as funcionalidades de listagem de diretórios;

Remover todas as funcionalidades e arquivos desnecessários;

Remover qualquer comentário, código de teste ou outra funcionalidade desnecessária em ambiente de produção;

Utilizar ferramenta de controle de versão;

Os painéis de administração não devem ficar disponíveis para acesso via internet;

As senhas default dos aplicativos devem ser desabilitadas ou alteradas;

As contas default dos aplicativos devem ser desabilitadas ou alteradas;

Não deve haver senhas configuradas em texto claro nos arquivos de configuração no servidor (ex. arquivos .conf, .xml, etc.).

Seção X - Da segurança em banco de dados

3.10. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto a segurança em banco de dados:

Utilizar validação de dados de entrada e em caso de falha, não executar o comando no banco de dados;

A aplicação deve possuir o mínimo de privilégio possível para acesso ao banco de dados;

As informações de conexão não devem ficar armazenadas na própria aplicação, devendo ser armazenadas em arquivo separado, com conteúdo criptografado e acesso somente a pessoal autorizado;

Não utilizar as contas default para administrar os bancos de dados;

As senhas dos usuários de conexão aos bancos de dados devem ser fortes, obedecendo aos parâmetros de senhas seguras.

Seção XI - Do gerenciamento de arquivos

3.11. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto ao gerenciamento de arquivos:

Limitar os tipos de arquivos que aceitos pela aplicação, realizando a validação pelo cabeçalho ao invés da extensão;

Os arquivos devem ser salvos em um local diferente de onde a aplicação está localizada;

Os caminhos completos dos arquivos não devem ser exibidos durante a transmissão ou armazenamento dos arquivos;

Os arquivos devem ser verificados por um antivírus antes de serem armazenados.

Seção XII - Das práticas gerais de codificação

3.12. O desenvolvimento de novos sistemas de informação deve seguir as seguintes práticas quanto às práticas gerais de codificação:

Sempre que possível, utilizar funções, bibliotecas e códigos já disponíveis e testados, ao invés de um novo código;

As aplicações devem contar com mecanismos que previnam condições de concorrência (raceconditions), como por exemplo, evitar requisições simultâneas;

Sempre realizar o tratamento dos dados adequadamente, antes de transferir as entradas dos usuários para qualquer função;

A geração e a alteração de código devem ser limitadas aos usuários privilegiados e deve se limitar o mínimo possível dentro da própria aplicação.

IV - Da propriedade intelectual

4. O direito autoral de Propriedade Intelectual de todo e qualquer código e tecnologias desenvolvidas pelo TJBA e para o TJBA, além dos demais serviços entregáveis (manuais de utilização, memorial descritivo, especificações funcionais internas, código fonte comentado, diagramas, fluxogramas, programa executável, etc.), a título universal e irretratável, são exclusivos do TJBA, consoante Lei nº 9.609/98 e 9.610/98.

V - Do acesso ao código-fonte

5. O acesso ao código-fonte das aplicações deve ser restrito somente aos desenvolvedores das aplicações.

5.1. As equipes da SETIM devem utilizar uma solução de repositório central de versões, onde somente pessoas autorizadas possuam acesso aos arquivos contendo os códigos-fonte de todas as aplicações. Esse repositório deve concentrar todos os códigos-fonte, pacotes de melhoria, scripts de bancos de dados, arquivos de novas versões, entre outros. A utilização de um repositório centralizado reduz o risco de que sejam aplicadas versões erradas em ambiente de produção, uma vez que tanto o desenvolvedor quanto o analista que for aplicar a melhoria em produção tenham visibilidade do mesmo arquivo, evitando a transferência de arquivos via e-mail ou sistema de chamados.

5.2. A ferramenta deve fornecer logs detalhados de quem fez acessos aos arquivos e quais foram as alterações realizadas. A ferramenta também deve dar a possibilidade de restaurar versões antigas dos arquivos alterados, fazendo o controle de versão dos arquivos.

VI - Dos testes de segurança

6.1. Após a conclusão do desenvolvimento de um novo sistema ou uma correção em um sistema já existente, a área de Segurança da Informação da COTEC deverá ser comunicada para que um teste de segurança mais aprofundado possa ser realizado. Essa comunicação visa ampliar a fase de testes de segurança e identificar falhas de programação que venham a comprometer a segurança do produto antes da conclusão do desenvolvimento, mesmo que o código esteja aderente aos requisitos do negócio. Entre os testes autorizados a serem realizados, estão os seguintes:

Injeção de código

Autenticação

Integração XML

Perfis de Acesso

Erros de configuração de segurança

Cross Site Script

Falta de logs e monitoramento

6.1.1. Além dos testes sugeridos anteriormente, outros testes poderão ser desenvolvidos pela equipe de Segurança da Informação baseado no conhecimento sobre o projeto que está sendo desenvolvido e nos requisitos de segurança solicitados.

6.2. Todo o procedimento realizado deve ser devidamente documentado e os resultados devem ser compartilhados com as equipes da SETIM e de desenvolvimento, para que os itens identificados como falhas sejam corrigidas. Após a sinalização da correção dos itens pela COSIS, os itens deverão ser testados novamente, para garantir a efetividade da correção proposta.

ANEXO VIII – Norma de Gerenciamento de Incidentes de Segurança

I - Das disposições gerais

1. Os incidentes de segurança da informação são caracterizados por colocar em risco um ou mais ativos de informação, seja uma ameaça confirmada, sob suspeita de estar ocorrendo ou a vir a ocorrer.

1.2. A gestão de incidentes de Segurança da Informação tem por objetivo:

Garantir a detecção de eventos e tratamento adequado quanto à categorização destes incidentes como “Incidente de Segurança da Informação”;

Garantir a correta avaliação e responder a esses incidentes da maneira mais adequada possível, minimizando os efeitos adversos;

Analisar e reportar as vulnerabilidades encontradas durante o processo de resposta a um Incidente de Segurança da Informação.

II - Dos meios de detecção de incidentes de segurança da informação

2.1. 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 usuário dos sistemas de informação que identificar uma situação atípica no ambiente, realizando uma denúncia para a equipe de Tecnologia da Informação, seja via abertura de chamado, e-mail, contato telefônico ou mesmo pessoalmente.

2.1.2. É dever de todo colaborador que ao identificar um incidente de segurança da informação ou estar sob suspeita de que um incidente esteja em curso, comunicar ao Service Desk, para que sejam realizadas as análises necessárias e as medidas adequadas sejam tomadas.

III - Da equipe de resposta a incidentes de segurança da informação

3. A equipe de resposta a incidentes de segurança da informação não é exclusiva para atender a esse tipo de incidente e poderá conter profissionais de diferentes especialidades dentro da Secretaria de Tecnologia da Informação e Modernização (SETIM) e inclusive ter o envolvimento da área usuária que realizou a denúncia, da área usuária que é responsável pelas informações contidas no ativo alvo e se necessário a alta administração da empresa.

IV - Do ciclo de vida de um incidente de segurança da informação

Seção I - Da triagem

4. Ao receber a informação de um incidente, independente do meio pela qual a informação tenha sido recebida, o analista da área de Segurança da Informação deverá fazer a avaliação inicial do incidente e, ao confirmar a informação como sendo um Incidente de Segurança da Informação, esse incidente deverá ser direcionado para a equipe de resposta a incidentes de segurança da informação. Após a confirmação em ser um Incidente de Segurança da Informação, ele deverá ser categorizado de acordo com seu risco potencial. Alguns cenários onde os incidentes detectados deverão ser tratados como Incidente de Segurança da Informação podem ser encontrados no ITEM 5.

Seção II - Da investigação

4.1. Nesta etapa, deve ser realizada a coleta de dados para uma avaliação, na tentativa de reduzir o impacto nas operações e identificar qual a causa do Incidente de Segurança da Informação.

4.2. Caso seja detectada uma ação potencialmente criminosa, a gestão deverá decidir se haverá envolvimento de equipes externas de análise forense ou mesmo de autoridades (força policial). Se for decidido por essa abordagem, a tratativa deverá seguir de modo diferente, pois toda a análise forense e produção de provas judiciais poderá ser comprometida em caso de ações equivocadas. Caso contrário, os processos de contenção, análise e recuperação podem seguir sem maiores necessidades de evidenciar legalmente as etapas realizadas e logs coletados.

Seção III - Da contenção

4.3. Na etapa de contenção, os danos devem ser mitigados, isso inclui retirar o ativo da rede, alterar regras de firewall, criar ACLs nos switches para bloquear o tráfego ou mesmo desligar o ativo para conter o ataque. As ações devem ser alinhadas com a gestão da SETIM e as áreas de negócio envolvidas, pois a retirada de um ativo da rede pode causar um impacto ao negócio maior do que o próprio Incidente de Segurança da Informação em si.

Seção IV - Da análise

4.4. Após a contenção, outras informações podem ser adquiridas na etapa de análise, possibilitando uma avaliação da causa raiz do Incidente de Segurança da Informação. Nesta etapa, é esperado que sejam encontradas informações como por exemplo:

O que foi afetado (disponibilidade, integridade e/ou confidencialidade)?

Quem causou o incidente?

Como foi causado?

Quando foi iniciado?

É possível identificar um motivo?

Seção V - Da Recuperação

4.5. Depois de entender o incidente de segurança ocorrido, sua causa raiz e seu modus operandi, a última etapa da Gestão de Incidentes de Segurança da informação deverá tomar ações que previnam que esse mesmo incidente ocorra novamente, como por exemplo, atualizações de sistemas, aplicações de patches de segurança, bloqueio de portas em firewall, criação de ACLs para segregação de redes, desativação de determinados serviços nos servidores, adição de controles de acesso físico e/ou quaisquer tipos de ações cabíveis e aprovadas pelas áreas de negócio afetadas.

Seção VI - Do relatório de incidente de segurança da informação

4.6. Quando da estabilização do ambiente, os responsáveis por responder ao incidente deverão criar um Relatório de Incidente de Segurança, que deverá ser o mais detalhado possível e deverá conter informações coletadas como: causa raiz, início do incidente, quais os ativos afetados, qual o impacto que teve para o negócio e maiores detalhes a respeito dos procedimentos adotados para a contenção do Incidente de Segurança da Informação e recuperação do serviço, bem como o plano de ação para evitar que esse mesmo Incidente de Segurança da Informação se repita. Também deverá constar neste relatório o número do chamado aberto para o tratamento deste incidente de segurança.

4.7. O Relatório de Incidente de Segurança da Informação deve ser criado em até 7 (sete) dias após a ocorrência do incidente, para que os detalhes possam ser relatados com maior clareza.

4.8. Os responsáveis pela SETIM deverão ser envolvidos na finalização do registro de incidente de segurança, para que esse incidente possa ser discutido com a equipe, a fim de analisar as melhorias apresentadas / plano de ação executado.

4.9. Após a implementação das melhorias propostas no Registro de Incidente de Segurança da Informação – RISI, o incidente de Segurança da Informação será considerado fechado.

V - Dos critérios de avaliação

5. Em virtude da necessidade de segregar os incidentes do dia a dia dos incidentes de segurança da Informação, os incidentes que se enquadrem nas categorias abaixo devem ser tratados como Incidente de Segurança da Informação:

Perda, roubo ou furto de ativos;

Exploração não autorizada de vulnerabilidade sistêmica em ativos de informação;

Comportamentos anormais em sistemas operacionais, bancos de dados e aplicativos diversos, que gere indisponibilidade, perda de confidencialidade ou perda de integridade das informações;

Vazamento de Informações confidenciais oficiais;

Vazamento de informações pessoais;

Compartilhamento de senhas;

Tentativas de invasão (interna ou externa) nos ativos de informação;

Disparo de SPAM através de ativo de informação interno;

Acessos não autorizados ao Datacenter;

Infecção massiva por vírus, ransomware e outros tipos de malware;

Indisponibilidade de serviços por ataques;

Tentativas de violação de acesso a recursos de rede e sistemas;

Ataques de Negação de Serviço (DoS, DDoS);

Uso impróprio dos ativos de tecnologia.

5.1. Outros cenários poderão surgir e serem considerados como incidente de segurança, com a avaliação da necessidade de se gerar um Relatório de Incidente de Segurança da Informação realizado pela área de Segurança da Informação da instituição.

VI - Dos demais incidentes

.6. Os incidentes que não forem considerados Incidentes de Segurança da Informação deverão ser tratados pela Central de Serviços, através de chamado.

ANEXO IV - Norma de Gerenciamento de Riscos de Tecnologia da Informação

I - Das disposições gerais

1.0. Para uma correta gestão de todo o ambiente computacional do TJBA é necessário que periodicamente seja realizada uma avaliação de riscos de tecnologia da informação, analisando tanto a parte técnica quanto a parte processual.

1.1. A área de Segurança da Informação deve realizar anualmente uma avaliação de riscos no TJBA.

1.1.2. A avaliação de riscos deverá ser alinhada com o Comitê Gestor de Segurança da Informação (CGSI), para que seja definido o escopo e profundidade das atividades que serão realizadas.

1.1.3. Após a aprovação do escopo por parte do CGSI, são iniciados os trabalhos de avaliação de risco para o processo, que inclui as seguintes fases:

Identificação e classificação dos ativos;

Identificação de ameaças;

Identificação de vulnerabilidades;

Análise da probabilidade de ocorrência;

Definição do impacto;

Determinação do risco;

Tratamento do risco;

Monitoramento do plano de ação.

II. Da avaliação dos riscos

II.1. Da identificação e classificação dos ativos

2.1. O início dos trabalhos de avaliação de riscos começa a partir da identificação e classificação dos ativos relacionados ao processo no qual será conduzida a avaliação.

2.1.2. O Departamento de Informática (DIN) é responsável por fornecer o inventário de equipamentos atualizado e com os responsáveis atrelados a cada ativo. Com os ativos identificados, a relevância, criticidade ou importância será definida, de modo qualitativo ou quantitativo, de acordo com o escopo da avaliação que está sendo realizada.

II.2. Da identificação de ameaças

2.2. Para que a análise de risco seja objetiva é necessário que sejam identificados quais as ameaças e a que ativos mapeados no item anterior estão expostas, focando nos cenários com maior probabilidade de ocorrerem. Com essa abordagem, é possível otimizar a realização da análise e aproximar o resultado aos cenários reais.

II.3. Da identificação de vulnerabilidades

2.3. Após a identificação das ameaças, o próximo passo da análise de risco é a atividade de análise de vulnerabilidades que podem ser exploradas pelas ameaças identificadas no passo anterior.

2.3.1. Essa análise não deve se ater somente aos ativos tecnológicos, mas também aos processos que envolvem tecnologia e que não podem ser analisados através de uma ferramenta, como, por exemplo, falhas nos processos de gestão de identidades, concessão de acesso, acesso físico, entre outros.

II.4. Da análise da probabilidade de ocorrência

2.4. Com as informações de ameaças, vulnerabilidades e os controles mitigatórios existentes em mãos, é possível estimar, baseado em dados históricos e estatísticas de mercado, qual a probabilidade de uma ameaça identificada explorar uma vulnerabilidade existente no ambiente.

2.4.1. Para que os dados históricos da instituição possam ser utilizados é necessário que o processo de gestão de incidentes de segurança da informação esteja implantado adequadamente, para que seja possível buscar por todos os incidentes ocorridos em um determinado período.

II.5. Da definição de impacto

2.5. Nesta etapa do processo, todas as informações coletadas anteriormente são utilizadas para calcular o resultado da materialização de uma ameaça.

2.5.1. Considerada a probabilidade de uma ameaça explorar uma vulnerabilidade, o impacto é calculado baseado no dano em potencial que o negócio viria a sofrer em caso de parada de um sistema, de roubo de uma informação ou de outro evento que ocorra.

II. 6. Da determinação do risco

2.6. A partir do resultado das etapas anteriores, é determinado um nível de risco ao qual a instituição está exposta a cada ameaça. Os critérios para determinação do risco devem ser baseados na Matriz de Risco de TI. O resultado da análise deve ser apresentado a Secretaria de Tecnologia da Informação e Modernização (SETIM), acompanhado de material complementar das etapas anteriores da avaliação de riscos.

III. Do tratamento do risco

3.0. Após a identificação dos riscos e seu grau de relevância para a instituição, é necessário definir um plano de ação para que o risco seja elevado a um nível aceitável.

3.1. As medidas para o tratamento dos riscos devem ser alinhadas inicialmente com a SETIM, com o objetivo de propor um plano de ação para cada risco identificado, após isso poderão ser tomadas as seguintes medidas:

Mitigação do risco: através da implementação de controles (sejam técnicos ou não), o risco é reduzido para um nível aceitável pela instituição, onde será necessário realizar uma monitoria periódica;

Transferência do risco: na impossibilidade de implementar controles mitigatórios, poderá ser realizada a transferência do risco para outra instituição, normalmente, uma companhia de seguros, que indenizará a instituição em caso de incidentes;

Eliminação do risco: o processo que gera o risco deixa de ser realizado, eliminando assim o risco associado a ele; e

Aceitação do risco: caso o custo ou esforço para a implementação de controles mitigatórios seja muito elevado, a instituição pode optar por aceitar o risco como inerente ao seu negócio. Neste caso, o CGSI deverá estar ciente da aceitação deste risco e devendo se responsabilizar pela decisão tomada de aceitar o risco.

3.2. Após a criação do plano de ação inicial com o tratamento para cada risco, o plano deverá ser apresentado ao CGSI, que poderá aceitar o plano sugerido ou determinar outras medidas para tratamento.

IV. Do monitoramento do plano de ação

4.0. Após a definição do plano de ação a ser tomado para a mitigação dos riscos, a área de Segurança da Informação deverá acompanhar o status de implementação das medidas, cobrando as áreas responsáveis pela correção.

4.1. A tarefa de acompanhamento deve ser realizada a cada quatro meses pela SETIM, a fim de que o status seja atualizado e o andamento das atividades seja apresentado para o CGSI.

V. Do risco residual

5. Após a evidência do tratamento do risco, o mesmo deverá ser recalculado, onde a tendência é que o novo valor de risco identificado seja menor do que o valor identificado inicialmente.

ACL (Access Control List):

É uma lista criada nos equipamentos de informática (ex.: firewall, switch, roteador e etc.) onde são definidos os usuários/equipamentos que têm autorização de acesso a um recurso em particular.

Aplicações de Negócio:

Aplicações que são utilizadas para realização de processos de negócios e podem estar hospedadas internamente ou em ambiente de T.I. provido por empresa terceira.

Área de Segurança da Informação:

Setor da Diretoria de Informática responsável pelo gerenciamento de segurança da informação no TJBA.

Autenticação:

É um processo que busca verificar a identidade digital do usuário de um sistema no momento em que ele requisita acesso em um programa ou computador.

Autenticidade:

Garante que a informação é verídica ou original.

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. Caso ocorra perda dos dados na origem, a cópia de segurança pode ser obtida a partir do dispositivo de destino. Termo genérico utilizado para definir uma cópia de segurança de dados armazenados ou mesmo o processo de criação de uma cópia de segurança.

Backup Full:

Tipo de backup que copia todas as informações dos serviços especificados e armazenados primariamente em servidores e armazenar em mídia externa.

Backups incrementais:

Tipo de backup que copia apenas as diferenças entre os backups realizados diariamente e o último backup executado.

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, bem como as tratativas que lhe foram dadas. Cada chamado possui um número único.

Cloud computing ou Computação em Nuvem:

É a entrega da computação como um serviço ao invés de um produto, onde recursos compartilhados, software e informações são fornecidas, permitindo o acesso através de qualquer dispositivo (computador, tablet, celular ou etc.) conectado à Internet.

Cookie:

Pequenos arquivos que as aplicações web gravam nos computadores para facilitar a identificação do usuário durante a navegação;

Colaborador:

Toda pessoa que exerça atividade, remunerada ou não, em função do Tribunal de Justiça do Estado da Bahia (TJBA). Ex: servidor com cargo permanente ou comissionado, prestador de serviço, terceiro, estagiário, consultor, temporário, voluntários, juízes, desembargadores e secretários.

Confidencialidade:

Garantia de que as informações só serão acessíveis as partes autorizadas.

Cross-site Scripting:

Tipo de vulnerabilidade em aplicações web que permite a execução de código malicioso na aplicação.

Custodiante:

Qualquer pessoa física ou jurídica, que detenha a posse de informação produzida por outrem.

DIN:

Diretoria de Informática e suas coordenações.

Disponibilidade:

Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Drive de Rede:

Espaço destinado a gravação de arquivos dentro de um Servidor de Arquivos corporativo do TJBA.

Equipamento:

Conjunto composto de partes físicas e lógicas (firmware/software) que funcionam de forma integrada para realizar uma ou mais das seguintes funções: processamento de informações, tarefas de automação, tarefas de comunicação.

Fail-secure:

Conceito onde mesmo na ocorrência de uma falha durante a execução de uma função, o sistema é mantido em estado seguro;

File Server:

Componente do ambiente de TIC, com função de servidor, que provê o armazenamento de arquivos eletrônicos. O usuário pode enviar arquivos para o servidor ou recuperar arquivos que estejam no mesmo.

Firewall:

É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Gestor da Informação:

Autoridade do TJBA ou dirigente de unidade responsável pela classificação da informação de sua competência.

Hardware:

Ativos de tecnologia físicos que suportam a prestação de serviços e o negócio do TJBA, tais como, estações de trabalho, smartphones, servidores, storages, links de dados e voz, roteadores, switches, entre outros.

Hash:

Algoritmo que valida a integridade de informações, mapeando os dados de comprimento variável para uma cadeira de caracteres de tamanho fixo.

HttpOnly:

É um atributo utilizado para mitigar o risco de um script acessar um cookie protegido no lado do cliente;

IMAP (Internet Message Access Protocol):

é um protocolo similar ao POP3 sendo, porém, superior em recursos. Usando o IMAP, as mensagens não são movidas, de modo que usuário pode ter acesso às mesmas mensagens em qualquer computador, usando webmail ou programa específico (denominado cliente) para acesso ao servidor de correio eletrônico.

Incidente de Segurança da Informação:

Qualquer evento que fuja da situação normal de utilização dos Sistemas de Informação, podendo ser uma violação ou uma ameaça de violação da Política de Segurança da Informação.

Informação:

Conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculada.

Informação Confidencial:

Informações cuja divulgação indiscriminada possa colocar em risco a segurança da sociedade ou do Estado. Por isso, apesar de serem públicas, o acesso a elas deve ser restringido por um período determinado.

Injeção SQL:

Tipo de ataque onde comandos de bancos de dados são inseridos em campos de formulários de aplicações web para aquisição de dados de maneira não-autorizada.

Integridade:

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Legalidade:

Todas os ativos de informação estão de acordo com a legislação nacional ou internacional vigentes.

Log:

Registro de um evento em um sistema computacional, que fica armazenado em um repositório e possibilita a análise de ações realizadas.

Malware:

O termo malware é proveniente do termo em inglês MALicious softWARE. Trata-se de um software destinado a se infiltrar em um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Exemplos: vírus de computador, worms, cavalos de Tróia, spywares.

Mídias de Retenção:

São mídias capazes de serem removidas do ambiente do objeto de cópia, ou que já estejam armazenadas em ambiente distinto desde a primeira gravação.

Mídias Removíveis:

Dispositivos que permitem a leitura e gravação de dados tais como: HD externo, CD, DVD, Pen Drive, cartão de memória, entre outros.

Mídias Sociais:

São ferramentas de colaboração online onde é possível ler, receber, criar, armazenar, enviar e compartilhar conteúdo digital com outras pessoas conectadas. Ex.: Twitter, Facebook, Flickr, Wikipédia, YouTube, Vimeo, LinkedIn, Google+, blogs, dentre outros.

Mídias Temporárias:

Uma mídia temporária é caracterizada por alta velocidade de cópia e restauração, geralmente sobre estrutura de discos e podem se manter no ambiente do objeto de cópia. Seus dados são regularmente sobrescritos, logo depois de movidos para uma mídia de retenção.

Modem USB:

É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como notebooks, netbooks, desktops, tablets, etc. objetivando conexão com a Internet. O modem USB recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para equipamentos compatíveis com a tecnologia 3G/4G.

Network Time Protocol (NTP):

Protocolo responsável por fazer a sincronia de horário entre os ativos da rede interna e uma fonte pública confiável.

Network-Dedicated:

Dispositivos de armazenamento que utilizam como mídia de transferência de dados uma rede de comunicação dedicada, não compartilhando a largura de banda com outros serviços oferecidos.

Network-Shared:

Dispositivos de armazenamento que utilizam como mídia de transferência de dados a rede de comunicação local, compartilhando a largura de banda com outros serviços oferecidos.

Nobreak:

É um sistema de alimentação secundário de energia elétrica que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia primária.

Patch crítico:

Atualização liberada emergencialmente onde, devido à criticidade e exposição causada pela vulnerabilidade que ele corrige, deve ser aplicada o mais rápido possível.

Patch tuesday:

Data em que a Microsoft lança suas atualizações. É sempre a segunda terça-feira de cada mês, ocorrendo sempre entre os dias 8 e 14.

Patch:

Em programação de computadores diz-se da correção de uma deficiência no desempenho de uma rotina ou programa existentes.

POP3:

Post Office Protocol version 3 (POP3):é um protocolo de comunicação que permite acessar mensagens eletrônicas existentes em uma caixa de correio, necessariamente movendo-as para o computador local.

Race Condition:

Estado onde duas ou mais funções concorrem com a execução entre si, como por exemplo, efetuar uma transição (função 1) antes da checagem de autorização (função 2) ser finalizada;

Restore:

Procedimento utilizado para restaurar no devido ambiente o conteúdo de uma cópia de segurança, recuperando assim os dados anteriormente armazenados.

Rótulo:

Registro que visa a identificar claramente a classificação da informação, no momento de sua produção.

Secure:

É um atributo que previne que os cookies sejam observados por usuários não-autorizados durante sua transmissão em texto claro;

Senha de Acesso:

Também denominada Senha ou Password. É um código secreto que o usuário precisa apresentar para ser validada em um processo de autenticação.

Serviços de Infraestrutura:

Serviços que suportam as atividades desempenhadas pelo TJBA.

Sistemas de Informação:

Sistemas implantados ou em fase de implantação, destinados ao atendimento das atividades instituição.

Smartphone (telefone inteligente, numa tradução livre do inglês):

É um telefone móvel com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional.

SMTP (Simple Mail Transfer Protocol):

É o protocolo usado no sistema de correio eletrônico na arquitetura Internet.

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.

Storages:

Hardware que contém espaços para vários discos rígidos, conectado aos servidores, a fim de armazenar os dados com segurança.

Switch:

É um equipamento que interliga os computadores em uma rede.

Transport Layer Security (TLS):

Protocolo de transmissão seguro via internet, utilizando certificados de segurança para garantir a integridade das informações.

Tokens:

Dado utilizado na comunicação de redes para identificar uma sessão de uma aplicação;

USB:

É um tipo de conexão "ligar e usar" (plug and play) que permite a conexão de periféricos sem a necessidade de desligar o computador.

Virtual patch:

Solução de segurança que protege um ativo bloqueando tráfego de rede malicioso que utilize uma vulnerabilidade baseada em uma atualização que ainda não foi aplicada ao ativo.

VPN:

Sigla para Virtual Private Network (Rede Virtual Privada). É uma tecnologia para criptografar os dados que são transferidos entre duas ou mais redes.

5ª Av. do CAB, nº 560, Salvador/BA - Brasil. CEP 41745-971. Fone: (71) 3372-5686/5689.