INSTITUTO FEDERAL DE
EDUCAÇÃO CIÊNCIA E TECNOLOGIA

NORMAS DE SEGURANÇA DA INFORMAÇÃO

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO (CGTI)

DEZEMBRO/2013

Rua do Rouxinol, Nº 115 / Salvador – Bahia – CEP: 41.720-052
Telefone: (71) 3186-0001. Email: cgti@listas.ifbaiano.edu.br
Site: http://www.ifbaiano.edu.br

Sumário

MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO

NORMAS DE SEGURANÇA DA INFORMAÇÃO

PRESIDENTE DA REPÚBLICA

Dilma Rousseff

MINISTÉRIO DA EDUCAÇÃO

Aloízio Mercadante

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO

Reitor

Sebastião Edson Moura

Diretor Executivo

Nilton de Santana dos Santos

Pró-reitorias

Administração e Planejamento

Eloivaldo Fagundes Pereira

Controle de Versão

Data	*Versão*	*Descrição*	*Autor*
02/08/2013	1.0	Edição do documento	Robson Ramos
05/08/2013	1.1	Revisão do documento	André Luiz Andrade Rezende
18/09/2013	1.2	Revisão do documento	Humberto Ataide Santiago Junior
08/12/2013	1.3	Formatação do documento	André Luiz Andrade Rezende

Ensino

Rosângela Maria de Sales Mota

Pesquisa e Inovação

Vandemberg Salvador de Oliveira

Extensão

Alberto Alves de Oliveira

Desenvolvimento Institucional

Jesusa Rita Fidalgo Sanchez

Diretorias Sistêmicas

Gestão de Pessoas

Miguel Rodrigues de Almeida

Gestão de Tecnologia da Informação

André Luiz Andrade Rezende

Unidades

Campus Catu

Alex Batista Dias

Campus Guanambi

Carlos Elizio Cotrim

Campus Santa Inês

Nelson Filho

Campus Senhor do Bonfim

Aécio José Araújo Passos Duarte

Campus Itapetinga

José Dionísio Borges de Macedo

Campus Teixeira de Freitas

Marcelito Trindade Almeida

Campus Valença

Francisco Harlei de Oliveira Mendonça

Campus Uruçuca

Euro Oliveira de Araújo

Campus Bom Jeus da Lapa

Ariomar Rodrigues dos Santos

Norma 01 - Responsabilidade dos Órgãos

1. Objetivo

Orientar a Reitoria e os *Campi*, do Instituto Federal de Educação, Ciência e Tecnologia Baiano (IF Baiano), quanto à utilização das Normas de Segurança da Informação.

2. Definições

Segurança da Informação: conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e ampliar as oportunidades de negócio;

Incidente de Segurança da Informação: representado por um simples ou por uma série de eventos de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;

Ativos de Tecnologia da Informação: estações de trabalho, servidores ou quaisquer outros equipamentos eletrônicos relacionados à Tecnologia da Informação, além de softwares, mídias e serviços de TI;

Gestão de Continuidade de Negócios: processo que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem, buscando desenvolver uma cultura organizacional capaz de responder e salvaguardar as informações e a reputação da instituição;

Gestão de Riscos: atividades coordenadas para direcionar e controlar a instituição no que se refere a riscos, incluindo, inclusive, análise e avaliação, tratamento, aceitação e comunicação dos riscos.

3. Diretrizes

3.1 Compete à Diretoria de Gestão de Tecnologia da Informação - DGTI, por intermédio do Núcleo de Segurança da Informação - NSI:

3.1.1 coordenar as atividades de Segurança da Informação, a exemplo de Gestão de Continuidade de Negócios, Gestão de Incidentes de Segurança da Informação e Gestão de Riscos, nos níveis estratégico e tático;

3.1.2 promover ações que assegurem que as estratégias relacionadas a Segurança da Informação estejam alinhadas com os objetivos de negócio de órgãos e entidades do Poder Executivo Federal;

3.1.3 prospectar as soluções de segurança existentes no mercado e avaliar sua adequação para o Instituto Federal Baiano;

3.1.4 avaliar o resultado do nível de segurança alcançado e propor medidas corretivas e preventivas;

3.1.5 manter a Alta Administração do IF Baiano informada sobre os assuntos relativos à Segurança da Informação;

3.1.6 coordenar as atividades operacionais relacionadas à Segurança da Informação a nível do IF Baiano;

3.1.7 prover suporte metodológico e apoio ao planejamento das atividades relacionadas a Segurança da Informação nos Campi e Reitoria do IF Baiano;

3.1.8 verificar, continuamente, se os *Campi* do IF Baiano estão atuando em conformidade com as diretrizes da Política e Normas de Segurança da Informação;

3.1.9 promover, periodicamente, programas de conscientização e capacitação em Segurança da Informação, bem como monitorar os seus resultados.

3.2 Compete a DGTI

3.2.1 fornecer as diretrizes estratégicas do negócio para orientar as atividades de Segurança da Informação;

3.2.2 acompanhar, periodicamente, a evolução dos indicadores de Segurança da Informação adotados no âmbito do Instituto;

3.2.3 apoiar, sugerir, garantir e implementar em sua área de atuação as ações de Segurança da Informação;

3.2.4 fazer cumprir a Política e Normas de Segurança da Informação;

3.2.5 reportar a ocorrência de incidentes de Segurança da Informação ao Comitê Gestor de Tecnologia da Informação - CGTI.

3.3 Caberá a DGTI analisar e dirimir as dúvidas sobre as Normas, e os casos omissos deverão ser encaminhados ao CGTI para exame.

4. Documento Relacionado

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

5. Data da Revisão

- 19/09/2013.

Norma 02 – Classificação da Informação

1. Objetivo

Estabelecer diretrizes que garantam que todas as informações, independente de seus meios de armazenamento ou transmissão, recebam níveis adequados de proteção e sejam classificadas com clara indicação do assunto, fundamento da classificação, indicação do prazo do sigilo e identificação da autoridade que a classificou, respeitando o princípio da observância da publicidade como preceito geral e do sigilo como exceção, conforme a Lei Federal nº 12.527, de 18 de Novembro de 2011 (Lei de Acesso à Informação Pública).

2. Definições

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da instituição, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

Informação Pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem; Proprietário da Informação: aquele que gera ou adquire a informação;

Custodiante da Informação: aquele que armazena, processa, veicula e trata a informação, mediante orientação dada pela classificação dada à informação e assume, em conjunto com o proprietário da informação, a responsabilidade pela proteção desta;

Usuário: qualquer colaborador seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa ou utiliza informações custodiadas ou de propriedade do IF Baiano em local ou jornada de trabalho deste último;

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

3. Diretrizes

3.1 Os sistemas de informação e os serviços de rede do IFBAIANO serão classificados em três níveis quanto à segurança:

I – Disponibilidade – indica o quanto um sistema de informação ou serviço de rede deve estar disponível para acesso do usuário. Quanto à disponibilidade, os sistemas de informação e os serviços de rede são classificados como:

1. **de alta disponibilidade**: com indisponibilidade máxima de 2h (duas horas) ininterruptas no período das 7 às 19h em dias úteis (assim considerados os dias com atividades administrativas nos setores da Administração Central do IFBAIANO) e 24h (vinte e quatro horas) ininterruptas fora deste período. São considerados sistemas e serviços de alta disponibilidade: o acesso a sistemas oficiais do Governo Federal pelos setores responsáveis, o correio eletrônico institucional e o *website* institucional (www.ifbaiano.edu.br);

2. **de média disponibilidade**: com indisponibilidade máxima de 4h (quatro horas) ininterruptas no período das 7h às 19h em dias úteis e 48h ininterruptas fora deste período. São considerados sistemas e serviços de média disponibilidade: todos os sistemas de informação (acadêmicos e administrativos) e os serviços de rede hospedados nos ativos e servidores de rede sob responsabilidade dos setores de TI de cada unidade e que não estão enquadrados como de alta disponibilidade;

3. **de baixa disponibilidade**: sem definição de tempo de indisponibilidade. São considerados sistemas e serviços de baixa disponibilidade: os sistemas de informação e serviços de rede não hospedados nos ativos e servidores de rede sob responsabilidade dos setores de TI de cada unidade e que não estão enquadrados como de alta disponibilidade;

II – Confidencialidade – indica a permissão de acesso à informação. Quanto à confidencialidade, os sistemas de informação e os serviços de rede são classificados como:

1. **confidenciais**: de acesso restrito a usuários autorizados nominalmente. São considerados sistemas e serviços confidenciais: todos os sistemas de informação (acadêmicos e administrativos), o correio eletrônico institucional, os repositórios de arquivos, os serviços de banco de dados, os módulos de administração e configuração dos sistemas e serviços de circulação restritos ou abertos;

2. **de circulação restrita**: de acesso permitido a todos os usuários cadastrados no domínio de rede, podendo haver diferenciação por perfil de usuário. São considerados sistemas e serviços de circulação restrita: serviços, aplicações e conteúdos institucionais direcionados aos usuários cadastrados (Intranet), modelos de documentos e formulários *web*, arquivos de uso geral, serviços de impressão;

3. **abertos**: de acesso livre apenas para leitura. São considerados sistemas e serviços abertos: *websites* e serviços de fornecimento de arquivos.

III – Integridade – indica o grau de importância de manutenção de cópias de segurança. Quanto à integridade, as informações e serviços de rede são classificados como:

1. **integridade alta**: que prevê redundância de gravação para recuperação integral da última informação armazenada em caso de sinistro, cópia de segurança diária e guarda de informações de datas anteriores. São considerados sistemas e serviços de alta integridade: todos os sistemas de informação (acadêmicos e administrativos) hospedados nos servidores sob responsabilidade dos setores de TI de cada unidade, o correio institucional e as configurações e *scripts* de serviços;

2. **integridade média**: que prevê cópia de segurança diária e guarda de informações de datas anteriores. São considerados sistemas e serviços de média integridade: os serviços de rede hospedados nos servidores sob responsabilidade dos setores de TI de cada unidade, que não estão enquadrados como de alta integridade;

3. **sem garantia**: que não prevê guarda de dados. São considerados sistemas e serviços sem garantia: os serviços, sistemas e informações não hospedados nos servidores sob responsabilidade dos setores de TI de cada unidade e que não possuem cópia de segurança diária em servidores sob responsabilidade dos setores de TI de cada unidade, os serviços e informações relacionados a alunos e visitantes, os arquivos guardados em sistemas que não são os servidores sob responsabilidade dos setores de TI de cada unidade (estações de trabalho, *pen drives*, disquetes e outros), demais informações não citadas anteriormente.

4. Competências

4.1 Usuário

- Classificar as informações , conforme as diretrizes desta norma.

4.2 Proprietário da Informação

- Determinar o nível de criticidade e a classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas pelos entes competentes.

4.3 Núcleo de Segurança da Informação - NSI

- Orientar o proprietário da informação quanto a classificação da informação;
- Observar o cumprimento desta Norma.

5. Documentos Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Lei Federal nº 12.527, de 18 de Novembro de 2011 – Lei Federal de Acesso à Informação Pública;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6. Data de Revisão

- 19/09/2013.

Norma 03 – Uso da Internet

1. Objetivo

Estabelecer as diretrizes de proteção relativas ao uso da *Internet* e de outras redes públicas de computadores, com o objetivo de reduzir o risco a que estão expostos os Ativos de Tecnologia da Informação do IF Baiano, tendo em vista que a *Internet* tem sido veículo de muitas ações prejudiciais às organizações, gerando perdas financeiras, perdas de produtividade, danos aos sistemas e à imagem da organização, entre outras consequências.

2. Definições

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre;

Internet: consiste de milhares de redes de computadores interconectadas mundialmente e que pela sua abrangência e facilidade de uso, tem sido usada como plataforma para a prestação de um crescente número de serviços;

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pelo IF Baiano em local ou jornada de trabalho para este último;

Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como as conexões com a *Internet, hardware* e *software;*

Incidente de Segurança da Informação: é indicado por um simples ou por uma série de eventos de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação.

3. Abrangência

Esta Norma se aplica a todos os usuários que fazem uso da *Internet,* permanente ou temporariamente, através dos recursos computacionais disponibilizados pelo IF Baiano, bem como os que utilizam a *Internet* como meio de comunicação através de conexão com a rede interna do instituto.

4. Diretrizes

4.1 Toda área de transferência de dados em computadores do IF Baiano acessível pela Internet e disponível publicamente para gravação deve ser limpa regularmente;

4.2 A informação obtida na Internet de forma livre e gratuita deve ser confirmada por fontes fidedignas antes de ser efetivamente usada;

4.3 O dirigente máximo de cada unidade do IF Baiano pode solicitar ao setor de TI de sua unidade, relatório técnico a cerca do conteúdo transmitido e armazenado nos computadores dentro de sua unidade.

4.4 Os Ativos de Tecnologia da Informação do IF Baiano, incluindo as conexões com a Internet, hardware e software, devem ser empregados na consecução dos seus objetivos institucionais, sendo vedada a sua utilização para outros fins, exceto para os casos explicitamente permitidos por esta norma;

4.5 Controles de Acesso a Serviços da Internet.

4.5.1 O acesso à Internet deve ser disponibilizado por meio de listas positivas ou negativas, cabendo a cada unidade definir a sua regra;

4.5.2 A permissão de acesso à Internet deve ser concedida através de uma Conta de Usuário que possibilite identificar, individualmente, seu proprietário, podendo o histórico de acesso, inclusive o conteúdo, ser monitorado, sem necessidade de notificação prévia, devendo ser armazenado por um período mínimo de 30 (trinta) dias, ressalva será feita para dias de evento e pela rede visitante de cada unidade, para esses momentos será registrado o endereço mac de cada equipamento.;

4.5.3 Não é permitido suprimir, omitir ou mascarar a identificação da Conta de Usuário a qualquer serviço da Internet, exceto para os serviços que permitem conexão anônima, não sendo permitido também o uso de mecanismos de dissimulação do usuário, como re-mailers, IP Spoofing, tradutores de URL e redes TOR, o uso desses serviços só é permitido para fins acadêmicos e com prévia autorização da UTIC, que terá a obrigação de notificar à DGTI.

4.5.4 A Administração do IF Baiano pode, sem aviso prévio, restringir o acesso a serviços da Internet, tais como sítios *Web*, redes de dados ponto-a-ponto e download de arquivos;

4.5.5 A possibilidade de acessar qualquer serviço da Internet não implica em autorização para acessá-lo;

4.6 Conexões de Rede com a Internet

4.6.1 É vedada a conexão entre qualquer rede de dados do IF Baiano e a Internet através de serviços de telecomunicações não autorizados pela área de TI da unidade;

4.6.2 É vedada a utilização de dispositivos de acesso à Internet não autorizados (3g e outros), em equipamentos pertencentes ao IF Baiano;

4.6.3 A comunicação entre computadores remotos e as redes do IF Baiano, através da Internet ou outra rede pública, preferencialmente deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pelo órgão responsável pela rede;

4.6.4 Toda a comunicação entre as redes do IF Baiano e a Internet ou qualquer outra rede pública deve passar por firewall institucional, configurado com política restritiva, com monitoramento dos fluxos de comunicação e com proteção contra ataques;

4.7 Uso Aceitável da Internet

4.7.1 É permitido o acesso a sites que sejam fontes de informação necessária à execução das atividades do IF Baiano;

4.7.2 É permitido o uso de serviços pessoais prestados através da Internet, tais como banco on-line, reservas de passagens, serviços de órgãos públicos, entre outros.

4.7.3 Não devem ser usados os recursos de "Salvar Senha" ou "Lembrar Senha", disponíveis na maioria das aplicações (*Thunder Bird, Outlook, Internet Explorer,* etc), devendo ser desmarcada sempre que for apresentada esta opção. Senhas não devem ser incluídas em nenhum outro processo de autenticação automática disponível, a única resalva são sistemas de armazenamento de senhas criptografados;

4.7.4 Quando estiver usando a Internet e verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site e abrir um incidente de Segurança da Informação em sistema disponibilizado pelo setor de TI;

4.7.5 Não é permitido o uso de aplicações ponto-a-ponto (*peer-to-peer*) para distribuição de arquivos, tais como *Kazaa, Napster, Emule* e correlatos, o uso desses serviços só é permitido para fins acadêmicos e com prévia autorização da UTIC, que terá a obrigação de notificar à DGTI.;

4.7.6 Não é permitido o uso de jogos *on-line*, o uso dos mesmos só é permitido para fins acadêmicos e com prévia autorização da UTIC, que terá a obrigação de notificar à DGTI.

4.7.7 Ressalvados os interesses da Administração do IF Baiano, não é permitido:

a) o acesso a conteúdos impróprios, que são aqueles relativos à pornografia, racismo, violência, incitação ao ódio/intolerância, invasão de computadores, entre outros;

b) a sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas do IF Baiano ou de qualquer outra organização, exceto quando autorizada pela área de tecnologia da informação do respectivo órgão ou entidade da Administração Pública;

c) o uso ou a posse de ferramentas de hardware e software para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela área de tecnologia da informação do IF Baiano.

4.8 Criptografia

4.8.1 Recomenda-se que toda a informação classificada como sigilosa, transmitida pela Internet, deve ser criptografada, conforme padrões de criptografia homologados pelo DGTI/NSI;

4.8.2 Informações que são alvo típico de criminosos, tais como senhas de sistemas e contas bancárias, números de cartões de crédito, entre outras, não devem ser publicadas na Internet ou transmitidas via Correio Eletrônico sem criptografia.

4.9 Legalidade

4.9.1 Sempre que as transações através da Internet ultrapassarem as fronteiras nacionais, devem ser observadas as legislações internacionais pertinentes;

4.9.2 A propriedade intelectual deve ser respeitada em qualquer atividade e sempre que os recursos computacionais do IF Baiano estiverem sendo usados. A reprodução ou encaminhamento de qualquer conteúdo protegido por direitos de propriedade requer a autorização do proprietário dos direitos autorais;

4.9.3 Sempre que informações obtidas da Internet forem usadas em documentos internos, a fonte deve ser citada;

4.9.4 A indicação de direitos reservados deve ser presumida para todo conteúdo disponível na Internet, a menos que contenha informação contrária, a exemplo do Creative Commons;

4.9.5 Usuários dos serviços de Internet do IF Baiano não devem obter, armazenar ou transmitir conteúdo ilegal, tais como software não licenciado, pornografia infantil, senhas, informações bancárias extraviadas, entre outros.

4.10 Download de Arquivos

4.10.1 Ressalvado os interesses do IF Baiano, não é permitido o download de filmes, músicas, vídeo *clips* ou conteúdos semelhantes relacionados a entretenimento;

4.10.2 O download de arquivos com grande volume de dados deve considerar as limitações da conexão com a Internet e, a unidade de TI local deve ser consultada sobre grande demanda de dados, de forma a equacionar uma maneira de não impactar no funcionamento da unidade (aplicação de limites de largura de banda para o download ou alteração do horário do mesmo para fora do horário normal de expediente);

4.10.3 O download e uso de softwares deve obedecer aos contratos estabelecidos com os fabricantes/fornecedores;

4.10.4 Todo arquivo deve ser submetido à verificação de software antivírus institucional antes de ser utilizado.

5. Competências

5.1 Diretoria de Gestão de Tecnologia da Informação – DGTI

5.1.1 disseminar e observar o cumprimento desta Norma.

5.2 Gerencia de Tecnologia da Informação – GETEC

5.2.1 prover os recursos necessários ao cumprimento desta Norma;

5.2.2 avaliar e homologar novos serviços de Internet antes de serem utilizados.

6. Documentos Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma 02 - Classificação da Informação;
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação;
- Norma 05 - Acesso e Utilização do Correio Eletrônico;
- Norma 07 - Intercâmbio de Informações;
- Norma 10 - Proteção Contra Código Malicioso;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

7. Data de Revisão

- 19/09/2013.

Norma 04 – Acesso aos Recursos de Tecnologia da Informação

1. Objetivo

Estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela Administração do IF Baiano.

2. Definições

Autenticação: processo de verificação que confirma se uma entidade ou um objeto é quem ou o que afirma ser, incluindo, em alguns exemplos, a confirmação da origem e da integridade das informações, tal como a verificação de uma assinatura digital ou da identidade de um utilizador ou de um computador;

Conta Genérica: credencial de acesso à rede que não identifica o usuário que a utiliza;

Conta de Usuário: credencial de acesso à rede ou sistemas, de uso pessoal, intransferível e de responsabilidade de seu usuário designado;

Credencial de Acesso: elemento utilizado para autenticar um usuário perante recursos de Tecnologia da Informação, tais como nome de usuário e senha, certificado digital, informação biométrica ou equivalentes;

Estação de Trabalho: todos os computadores e equipamentos correlatos do IF Baiano, inclusive dispositivos móveis;

Login/Logon: processo de autenticação com o objetivo de permitir o uso de um sistema computacional ou recursos de rede de forma segura;

Logoff: processo de encerramento do uso de um sistema computacional ou recursos de rede, removendo as credenciais de acesso;

Recursos de Tecnologia da Informação: estações de trabalho, servidores, redes, sistemas, serviços, banco de dados e dispositivos de interconexão;

Rede: estações de trabalho, servidores e outros dispositivos interligados que compartilham informações ou recursos do IF Baiano;

Token: dispositivo portátil utilizado para incrementar a segurança do processo de logon;

Usuário: qualquer colaborador seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pelo IF Baiano em local ou jornada de trabalho para este último.

3. Diretrizes

3.1 Concessão de Acesso

3.1.1 A licença para a utilização dos recursos de Tecnologia da Informação é uma concessão do IF Baiano aos usuários que necessitem deles para desempenhar suas funções. A utilização poderá ser monitorada em tempo real e a licença poderá ser suspensa a qualquer momento por decisão do Gestor da área do usuário, da área de tecnologia da informação do órgão ou entidade ou da Gerencia de Tecnologia - GETEC, de acordo com os exclusivos critérios destes, visando evitar perda de produtividade e riscos de segurança;

3.1.2 O acesso à consulta ou utilização dos recursos de Tecnologia da Informação é permitido após a identificação do usuário, somente por meio de suas próprias credenciais de acesso;

3.1.3 As credencias de acesso aos recursos de Tecnologia da Informação são pessoais, intransferíveis e de responsabilidade exclusiva do usuário, exceto para aqueles recursos que não suportarem a criação de credenciais individuais;

3.1.4 Toda solicitação, alteração, bloqueio e desbloqueio de acesso aos recursos de Tecnologia da Informação ou aos sistemas deve ser documentada;

3.1.5 O Gestor da área do usuário deve informar à área de tecnologia da informação da instituição ao administrador do recurso de Tecnologia da Informação todos os direitos de acesso que o usuário deve possuir;

3.1.6 O setor de recursos humanos da unidade deve informar ao setor de TI sobre nomeações, remoções, suspensões e exonerações dos usuários;

3.1.7 É expressamente proibida qualquer tentativa de acesso não autorizado aos recursos de Tecnologia da Informação;

3.1.8 A utilização de contas genéricas deve ser limitada ao estritamente necessário.

3.2 Conexão de Equipamentos

3.2.1 Somente dispositivos autorizados pela área de tecnologia da informação do órgão (Reitoria ou Campus) poderão ter acesso aos recursos de rede do IF Baiano.

3.3 Gerenciamento de Senhas

3.3.1 A elaboração de senhas para acesso à rede ou aos sistemas deve ser realizada conforme procedimento estabelecido pela área de tecnologia da informação da instituição, o qual deve prever troca periódica de senhas, senhas de difícil dedução e bloqueio automático da sessão por inatividade;

3.3.2 Todas as contas de usuário devem ter suas senhas alteradas no primeiro *logon* na rede, para assegurar sua confidencialidade;

3.3.3 Os critérios para elaboração, manutenção e gerenciamento dos acessos devem levar em consideração a criticidade das informações e as necessidades dos processos de negócio envolvidos.

3.4 Análise Critica

3.4.1 Os direitos de acesso dos usuários à rede e aos sistemas devem ser revisados periodicamente;

3.4.2 Os direitos de acesso dos usuários em afastamento definitivo da organização devem ser revogados;

3.4.3 Os direitos de acesso dos usuários em afastamento temporário devem ser suspensos no período da ausência.

4. Competências

4.1 Área de Tecnologia da Informação

4.1.1 administrar os acessos à rede e aos sistemas IF Baiano;

4.1.2 elaborar procedimento de gerenciamento de senhas em consonância com a criticidade das informações e as necessidades dos processos de negócio envolvidos.

4.2 Gestor do RH da unidade (NAGP/DGP)

4.2.1 comunicar à área de tecnologia da informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos;

4.3 Gestor da área do Usuário

4.3.1 comunicar à área de tecnologia da informação do órgão ou entidade sempre que tomar ciência de direitos de acesso desnecessários à execução das atividades por parte de seus subordinados ou de terceiros.

4.4 Usuário

4.4.1 manter sigilo da senha de acesso à rede e aos sistemas, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de acesso;

4.4.2 não compartilhar com terceiros sua credencial de acesso à rede ou aos sistemas;

4.4.3 informar ao seu Gestor quando forem identificados direitos de acesso desnecessários à execução das suas atividades profissionais;

4.4.4 bloquear sua estação de trabalho ou efetuar *logoff* da rede sempre que se ausentar de sua área de trabalho;

4.4.5 comunicar, imediatamente, à área de tecnologia da informação do órgão ou entidade qualquer ocorrência de perda ou avaria de dispositivos adicionais de autenticação, tais como tokens, smartcards e outros.

5. Documento Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma 03 - Uso da Internet;
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6 . Data de Revisão

- 19/09/2013.

Norma 05 – Acesso e Utilização do Correio Eletrônico

1. Objetivo

Definir as diretrizes de acesso e utilização segura do Correio Eletrônico disponibilizado pelo IF Baiano.

2. Definições

E-mail: forma reduzida para E(lectronic) Mail - Correio Eletrônico;

Hiperlink: palavras ou endereços em destaque de uma página da Internet ou mensagem de Correio Eletrônico que, ao serem clicadas, efetuam o direcionamento para outra parte do texto da mensagem ou página da Internet;

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral, que utiliza os recursos de Tecnologia da Informação disponibilizados pelo IF Baiano em local ou jornada de trabalho para este último;

Webmail: é um interface da Internet que permite consultar e enviar Correio Eletrônico (E-mail).

3. Diretrizes

3.1 O serviço de Correio Eletrônico corporativo é uma concessão do IF Baiano, sendo assim, seu uso é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens não relacionadas às atividades profissionais, que contenham:

3.1.1 assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem da organização;

3.1.2 temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

3.1.3 fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da organização.

3.2 As permissões de acesso a serviços de e-mail particulares, tais como webmail, podem ser estabelecidas e gerenciadas pela área de tecnologia da informação do órgão ou entidade e pelas áreas de negócio, em função dos interesses do IF Baiano;

3.3 O acesso ao Correio Eletrônico corporativo se dá pelo conjunto "Identificação do Usuário e Senha", que é pessoal e intransferível;

3.4 O endereço de e-mail disponibilizado ao usuário é de uso pessoal e intransferível e de responsabilidade do mesmo. Portanto, é terminantemente proibido suprimir, modificar ou substituir a identidade do remetente ou destinatário de uma mensagem do Correio Eletrônico;

3.5 Havendo indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer das vedações constantes deste ou de outro ato normativo, a área de tecnologia da informação da instituição responsável pela administração do Serviço de Correio Eletrônico adotará, imediatamente, medidas para a apuração dessas irregularidades, utilizando-se dos meios e procedimentos legalmente previstos;

3.6 A disponibilização do Correio Eletrônico pode ser suspensa a qualquer momento por decisão do Gestor da área do usuário ou da área de tecnologia da informação da instituição;

3.7 As concessões e revogações de acesso ao serviço de Correio Eletrônico devem ser autorizadas pelo Gestor da área do usuário por meio de uma solicitação de serviço à área de tecnologia da informação do instituto;

3.8 Os anexos das mensagens de Correio Eletrônico poderão ser bloqueados quando oferecerem riscos à Segurança da Informação;

3.9 A abertura de mensagens de remetentes desconhecidos, externos ao IF Baiano, deve ser avaliada, especialmente quando houver dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou hiperlinks para endereços externos não relacionados às atividades profissionais em curso;

3.10 A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de Spam. Cabe à área de tecnologia da informação da instituição estabelecer tal limite, bem como acordar com as áreas de negócio as eventuais exceções, de acordo com os interesses do IF Baiano;

3.11 Limites de armazenamento das caixas de Correio Eletrônico devem ser estabelecidos pela área de tecnologia da informação do Instituto, considerando as necessidades dos processos de negócio que o serviço de Correio Eletrônico suporta, bem como limitações técnicas aplicáveis.

4. Diretrizes

4.1 Área de Tecnologia da Informação

4.1.1 conceder, suspender e revogar os acessos ao serviço de Correio Eletrônico;

4.1.2 administrar as funcionalidades e a segurança do serviço de Correio Eletrônico.

4.2 Gestor da Área do Usuário

4.2.1 comunicar à área de tecnologia da informação do Instituto todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos.

4.3 Usuário

4.3.1 responder pelo uso adequado dos serviços e recursos de Correio Eletrônico a ele disponibilizados, nas suas mais diversas formas de acesso, inclusive por meio de dispositivos móveis, em consonância com esta Norma.

5. Documentos Relacionados

- A NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma 03 - Uso da Internet;
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação;
- Norma 10 - Proteção Contra Código Malicioso;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6. Data de Revisão

- 19/09/2013.

Norma 06 – Contabilização de Ativos de Tecnologia da Informação

1 Objetivo

Definir as diretrizes para a contabilização adequada dos Ativos de Tecnologia da Informação no âmbito do IF Baiano.

2 Objetivo

Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação;

Estação de Trabalho: todos os microcomputadores e equipamentos correlatos do IF Baiano, inclusive dispositivos móveis;

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso;

Incidente de Segurança da Informação: indicado por um simples ou por uma série de eventos de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias flash, discos removíveis, CD, DVD, mídia impressa, entre outros;

Shareware: programa disponível publicamente para avaliação e uso experimental, mas, cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. *Shareware* é distinto de freeware, no sentido de que um software *shareware* é comercial, embora em termos e preços diferenciados em relação a um produto comercial convencional;

Software Livre: denominação dada a determinado software cujo código-fonte é de acesso público;

Usuário: qualquer colaborador seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que utiliza Ativos de Tecnologia da Informação disponibilizados pelo IF Baiano em local ou jornada de trabalho para este último.

3 Objetivo

3.1 As informações e os Ativos de Tecnologia da Informação de propriedade do IF Baiano devem ser utilizados exclusivamente para os seus interesses, podendo ser monitorados a qualquer tempo;

3.2 Os Ativos de Tecnologia da Informação devem ser inventariados e identificados de forma única;

3.3 Os Ativos de Tecnologia da Informação devem ser classificados em função de sua relevância para o processo de negócio a que se destinam. Esta relevância deve ser considerada em eventuais análises de riscos;

3.4 Os Ativos de Tecnologia da Informação devem ser, sempre que possível, relacionados a um usuário, responsável por sua utilização;

3.5 O padrão de configuração (*hardware e software*) dos Ativos de Tecnologia da Informação é definido pela área de tecnologia da informação do Instituto e não deve ser modificado sem sua autorização;

3.6 Os itens que compõem conjuntos de ativos não podem ser modificados sem a autorização da área de tecnologia da informação dos órgãos e entidades;

3.7 Somente softwares licenciados e homologados devem ser utilizados;

3.8 Os inventários (*hardware e software*) devem ser atualizados apropriadamente sempre que Ativos de Tecnologia da Informação forem descartados;

3.9 As mídias contendo as cópias de segurança (backup) devem ser catalogadas e armazenadas por tempo compatível com as necessidades dos processos de negócio;

3.10 A utilização de software que não seja de propriedade do IF Baiano ou licenciado para o mesmo, pode, além de configurar crime de pirataria conforme Lei N° 9.609, de 19 de fevereiro de 1998, interferir na contabilização dos ativos.

4 Objetivo

4.1 Diretoria de Gestão de Tecnologia da Informação

4.1.1 contabilizar os Ativos de Tecnologia da Informação de forma a garantir sua conformidade com esta Norma.

4.2 Gerência de Tecnologia da Informação - GETEC

4.2.1 observar o cumprimento desta Norma.

4.3 Usuário

4.3.1 utilizar os Ativos de Tecnologia da Informação em conformidade com esta Norma;

4.3.2 notificar, através de abertura de incidente de Segurança da Informação, sempre que identificar dano, roubo, perda ou modificações indevidas em um Ativo de Tecnologia da Informação.

5 Documentação Relacionados

- Norma 04 – Acesso aos Recursos de Tecnologia da Informação;
- Norma 06 – Gerenciamento de Incidentes de Segurança da Informação;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6 Data de Revisão

- 20/09/2013.

Norma 07 - Intercâmbio de Informações

1 Objetivo

Definir as diretrizes de segurança na troca de informações e *softwares* internamente ao IF Baiano e/ou com quaisquer entidades externas.

2 Definições

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre;

e-PING: Padrões de Interoperabilidade de Governo Eletrônico – define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias flash, discos removíveis, CD, DVD, mídia impressa, entre outros;

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que utiliza informações ou sistemas de informação de propriedade do IF Baiano, em local ou jornada de trabalho deste último;

Virtual Private Network (VPN): Rede virtual privada com uso de criptografia para garantir a confidencialidade das informações trafegadas em uma rede pública.

3 Diretrizes

3.1 Diretrizes Gerais

3.1.1 A troca de informações entre os usuários deve ser suportada por acordos formalizados e documentados, contendo, quando aplicável, cláusulas de preservação da privacidade de dados pessoais, direitos autorais, preservação de bens patrimoniais, sigilo e não divulgação;

3.1.2 A construção e troca de arquivos entre os usuários deve observar os padrões da e-PING.

3.1.3 As informações classificadas como sigilosas gravadas em mídia removível devem utilizar solução de criptografia;

3.1.4 Toda informação sigilosa deve receber o tratamento adequado conforme descrito na Norma de Classificação da Informação;

3.1.5 Procedimentos de recepção de fac-símiles, impressão de documentos, abertura de correio e distribuição de correspondência devem ser estabelecidos de forma a prevenir o acesso não autorizado à informação;

3.1.6 Ações de conscientização dos usuários devem incluir a observância das necessidades de segurança ao se efetuar conversações, inclusive as telefônicas, sobre assuntos restritos e confidenciais em locais públicos, em escritórios abertos ou mesmo em reuniões realizadas em sala sem a devida adoção dos requisitos de segurança;

3.1.7 Mecanismos devem ser implementados para proteger as informações associadas aos sistemas de informação dos negócios, entre outros:

a) proteção contra interceptação e gravação de chamadas telefônicas ou de teleconferências, garantido a confidencialidade das chamadas;

b) o acesso à rede corporativa ou a Intranet, por meio da Internet, deve utilizar solução de criptografia (VPN - Virtual Private Network);

c) procedimento de retenção de cópias de segurança (backup) das informações mantidas nos sistemas, bem como sua recuperação e contingência;

d) restrição de acesso a informações de trabalho compatível às atividades do usuário através do gerenciamento de perfis de acesso;

e) proteção contra código malicioso, conforme Norma de Proteção Contra Código Malicioso;

f) procedimentos para o uso de comunicação sem fio, levando em conta os riscos particulares envolvidos;

g) as mensagens confidenciais, enviadas pelo Correio Eletrônico, devem utilizar solução de criptografia.

3.2 Mídias em Trânsito

3.2.1 Devem ser adotados transporte e serviço de mensageiro confiável e preferencialmente estabelecer um contrato de sigilo e confidencialidade com esse serviço;

3.2.2 Mecanismos de proteção contra danos físicos durante o transporte das mídias removíveis devem ser adotados, considerando as recomendações do fabricante das mídias;

3.2.3 A entrega dos documentos e das mídias removíveis, contendo informações sigilosas, deve ser registrada em sistema eletrônico de protocolo.

4 Competências

4.1 Área de Tecnologia da Informação

4.1.1 prover recursos para garantir a troca adequada de *software*, de informações armazenadas e transmitidas por meio eletrônico.

4.2 Usuário

4.2.1 cumprir as diretrizes desta norma.

5 Documentos Relacionados

- Norma 02 – Classificação da Informação;
- Norma 05 – Acesso e Utilização do Correio Eletrônico;
- Norma 10 – Proteção contra Código Malicioso;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6 Data de revisão

- 20/09/2013.

Norma 08 – Segurança em Terceirização e Prestação de serviços

1 Objetivo

Estabelecer diretrizes para implementar e manter o nível apropriado de Segurança da Informação e de entrega de serviços nos acordos firmados entre o IF Baiano e terceiros.

2 Definições

Incidente de Segurança da Informação: indicado por um simples ou por uma série de eventos de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;

Parceiro: qualquer entidade pública ou privada, organizações não governamentais ou instituições sem fins lucrativos com a qual se estabeleça uma relação de cooperação mútua;

Terceiro: qualquer parceiro, fornecedor ou prestador de serviço que acesse informações ou utilize recursos de Tecnologia da Informação disponibilizados pelo IF Baiano.

3 Diretrizes

3.1 Contratos firmados entre o IF Baiano e prestadores de serviço devem incluir acordos que definam os níveis de entrega de serviços, contemplando, entre outros:

3.1.1 definição explicita das responsabilidades e direitos legais do IF Baiano, da Prestadora de Serviços e dos profissionais envolvidos;

3.1.2 definição explícita dos direitos de propriedade dos produtos gerados;

3.1.3 aceite obrigatório de toda a Política de Segurança da Informação do contratante;

3.1.4 acordos de confidencialidade entre ambas as partes;

3.1.5 acordos de confidencialidade entre o terceiro e seus funcionários e subcontratados;

3.1.6 limitação do acesso apenas aos ativos e informações necessários à execução de suas atividades;

3.1.7 níveis de segurança durante os períodos de transição;

3.1.8 nível de capacidade técnica, logística e administrativa necessária do terceiro para prestar os serviços contratados;

3.1.9 planos para garantir os níveis de continuidade de serviços acordados após falhas severas nos serviços ou desastres;

3.1.10 acordos de nível de serviço (SLA), com indicadores adequados à natureza do contrato;

3.1.11 informação de que os serviços prestados poderão ser auditados.

3.2 Os serviços de terceiros, prestados ao IF Baiano devem ser monitorados e analisados criticamente de forma regular, a fim de garantir a aderência entre os termos de Segurança da Informação e as condições dos acordos, além de permitir o gerenciamento adequado de problemas e Incidentes de Segurança da Informação.

3.3 Devem ser executadas auditorias periódicas nos serviços de terceiros, contemplando:

3.3.1 níveis de desempenho de serviço para verificar aderência aos acordos;

3.3.2 relatórios de serviços produzidos por terceiros;

3.3.3 registros dos incidentes de Segurança da Informação e de sua respectiva análise crítica, tanto pelo terceiro quanto pelo órgão ou entidade, como requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiam;

3.3.4 trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigação de falhas e interrupção relativas ao serviço.

3.4 Um processo de gerenciamento de mudanças deve ser elaborado para os serviços prestados por terceiros a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos. Este processo deve contemplar:

3.4.1 melhoria dos serviços correntemente oferecidos;

3.4.2 desenvolvimento de quaisquer novas aplicações ou sistemas;

3.4.3 modificações ou atualizações das políticas e procedimentos;

3.4.4 novos controles para resolver os incidentes de Segurança da Informação e melhoria da segurança;

3.4.5 mudanças e melhorias em redes;

3.4.6 uso de novas tecnologias;

3.4.7 adoção de novos produtos ou novas versões;

3.4.8 novas ferramentas e ambientes de desenvolvimento;

3.4.9 mudanças de localização física dos recursos de serviços;

3.4.10 mudanças de fornecedores;

3.4.11 mudanças de contratos.

4 Competências

4.1 Áreas de Negócio

4.1.1 administrar os contratos sob sua responsabilidade;

4.1.2 monitorar e aprovar periodicamente as atividades dos prestadores de serviços, quanto à qualidade e eficiência;

4.1.3 avaliar regularmente o direito de acesso dos prestadores de serviço sob sua responsabilidade;

4.1.4 comunicar infrações aos acordos de segurança estabelecidos por meio de incidentes de Segurança da Informação;

4.1.5 auditar periodicamente os serviços de terceiros.

4.2 Área de Tecnologia da Informação

4.2.1 definir, junto as áreas envolvidas, os níveis de entrega de serviços adequados e os requisitos necessários para garantia da segurança das informações;

4.2.2 implementar um processo de gerenciamento de mudanças em recursos de Tecnologia da Informação para serviços de terceiros.

5 Documentos Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012;
- Norma 02 - Classificação da Informação;
- Norma 07 - Intercâmbio de Informações.

6 Data de revisão

- 20/09/2013.

Norma 09 – Desenvolvimento e Manutenção de Aplicações

1. Objetivo

Estabelecer as diretrizes que regulamentam a segurança para o processo de desenvolvimento e manutenção de *software* no âmbito do IF Baiano.

2. Definições

Artefato de Software: item criado como parte da definição, manutenção ou utilização de um processo de software, incluindo, entre outros, descrições de processos, planos, procedimentos, especificações, projetos de arquitetura, projeto detalhado, código, documentação para o usuário;

Base de Dados: conjunto de dados organizados de forma a servir de base para que o usuário processe e recupere informações;

Gestão de Configuração: conjunto de procedimentos técnicos e gerenciais que são definidos para identificação de Ativos de Tecnologia da Informação e para a gestão de suas alterações;

Rastreabilidade: capacidade de acompanhamento e registro de todos os eventos e movimentações ocorridas, desde a criação da informação até o seu descarte;

Usuário: qualquer colaborador, seja ele servidor público, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que utiliza os serviços de rede ou sistemas de informação disponibilizados pela Administração Pública Estadual em local ou jornada de trabalho para este último.

3. Diretrizes

3.1 Disposições Gerais

3.1.1 Pelo menos 1 (uma) metodologia deve ser estabelecida para todo desenvolvimento ou manutenção, com base nas melhores práticas de mercado, contemplando, entre outros:

a) planejamento;

b) análise de requisito;

c) projeto;

d) codificação;

e) revisão;

f) compilação;

g) teste.

3.1.2 Todo desenvolvimento ou manutenção de software deve ser formalmente autorizado.

3.1.3 Para todo desenvolvimento ou manutenção de software deve ser realizada uma análise de impacto.

3.1.4 Toda alteração de escopo de desenvolvimento ou manutenção de software deve ser documentada e formalmente autorizada.

3.1.5 Todas as ferramentas de desenvolvimento devem ser homologadas e licenciadas.

3.1.6 Todo projeto de software deve conter um documento de especificação de segurança que descreva seus objetivos de segurança, os quais devem, entre outros, contemplar:

a) o mecanismo de autenticação do usuário, que deve utilizar senhas com métrica mínima e exigir do usuário a troca periódica da senha;

b) o mecanismo de autenticação do usuário, que deve bloquear o acesso após número definido de tentativas de login com falha;

c) a verificação da senha por meio de mecanismo que impeça fraudes de repetição, interceptação ou quebra de integridade na comunicação entre o cliente e o servidor;

d) a escolha da senha por novos usuários sem a interferência do pessoal de apoio ou o recebimento pelos mesmos, de uma senha inicial que precise ser trocada;

e) o armazenamento da senha pelo sistema, de forma criptografada e irreversível;

f) a uniformidade do controle de acesso em todo o sistema, utilizando-se uma única rotina de verificação;

g) a realização do controle de acesso na camada mais próxima possível dos dados;

h) o registro, pelo sistema, dos eventos significativos para a segurança, principalmente, inicio e fim do mecanismo de auditoria;

i) o registro, pelo sistema, das falhas de login, indicando o número de tentativas;

j) o registro, pelo sistema, da criação e remoção de usuários, bem como da atribuição e da remoção de direitos do usuário;

k) a proteção da trilha de auditoria contra remoção e alteração por parte de todos os usuários, exceto dos administradores de auditoria;

l) a capacidade de tolerância do sistema à falhas e retorno a operação;

m) a inexistência, em aplicações web, de dados sensíveis em campos ocultos ou cookies;

n) a realização das verificações e validações de segurança no servidor, em aplicações web;

o) o acesso aos desenvolvedores apenas aos códigos fontes necessários para a alteração, quando autorizados pelo superior imediato;

p) a maior semelhança possível do ambiente de homologação ao ambiente de produção;

q) a exigência de que os aplicativos só passem do desenvolvimento para a homologação após verificação da existência e adequação de sua documentação;

r) a existência de documentação de instalação, configuração e operação do sistema, ressaltando os aspectos de segurança, que deve ser mantida atualizada.

3.1.7 Requisitos funcionais, não funcionais e de domínio devem ser especificados e documentados, bem como as manutenções necessárias, considerando os requisitos de segurança definidos no desenvolvimento do sistema.

3.1.8 A especificação dos requisitos deve ser elaborada em conjunto com a área de negócio solicitante da demanda.

3.1.9 Um mecanismo de controle de versão deve ser implementado durante o processo de desenvolvimento e manutenção de software.

3.1.10 Deve existir um programa de conscientização em Segurança da Informação para todos os usuários envolvidos nos processos de desenvolvimento de aplicações.

3.1.11 Devem existir mecanismos de verificação de vulnerabilidades no código fonte durante o processo de desenvolvimento e manutenção de software.

3.1.12 Incidentes de segurança devem ser abertos quando vulnerabilidades forem identificadas durante o processo de desenvolvimento e manutenção de software.

3.1.13 O acesso aos códigos fontes deve ser controlado e restrito aos desenvolvedores envolvidos, em seus respectivos projetos.

3.1.14 Os códigos fontes não devem conter identificações e/ou senhas de acesso às bases de dados, sejam elas de teste, de homologação ou de produção.

3.1.15 Ambientes de desenvolvimento e testes, de homologação e de produção devem ser isolados entre si.

3.1.16 Um processo de gestão de configuração deve ser implementado e deve abranger todo o processo de desenvolvimento e manutenção.

3.2 Todo software que implique em manipulação de dados deve ser desenvolvido com controle de acesso lógico. Mecanismos adicionais que possibilitem a rastreabilidade das operações efetuadas devem ser considerados em casos de manipulação de dados sensíveis.

3.3 Desenvolvimento Terceirizado

3.3.1 Todos os contratos com terceiros devem contemplar cláusulas de sigilo e confidencialidade.

3.3.2 Os produtos desenvolvidos externamente devem obedecer a padrões e metodologias homologadas, além de atender aos requisitos funcionais, não funcionais, de domínio e de segurança definidos.

3.3.3 O contrato de desenvolvimento de produtos com terceiros deve prever, no mínimo, os artefatos de software a serem entregues em cada fase, a validação, o procedimento de aceite final e o período de garantia.

3.4 Teste

3.4.1 Procedimentos de testes no software devem ser definidos e utilizados para todo desenvolvimento ou manutenção realizados, e devem contemplar, entre outros, controles tais como:

a) validação de dados de entrada;

b) controle de processamento interno;

c) integridade de mensagens;

d) validação de dados de saída.

3.4.2 Os testes devem validar os mecanismos de segurança especificados no desenvolvimento ou na manutenção do software.

3.4.3 Os testes de aceitação do software devem ser realizados por uma equipe diferente da equipe desenvolvedora, que deve ser composta por usuários da área de desenvolvimento e da área de negócio solicitante.

3.4.4 A utilização de dados de produção em ambiente de testes deve ser autorizada formalmente.

3.4.5 As informações contidas na base de dados de ambiente de produção, se utilizadas para testes, devem sofrer alterações, de modo a preservar sua confidencialidade.

3.5 Aceitação de Software

3.5.1 Os artefatos de software, provenientes de desenvolvimento ou manutenção, devem ser homologados antes de serem utilizados em ambiente de produção.

3.6 Mudanças Técnicas no Ambiente de Produção

3.6.1 As atualizações de configuração no ambiente de produção devem ser realizadas, inicialmente, em ambiente de teste e, todo software deve ser analisado criticamente, considerando os seguintes aspectos:

3.7 Implantação

3.7.1 Os produtos homologados devem ser implantados em ambiente de produção, por meio de procedimentos técnicos definidos pela área de tecnologia da informação do órgão ou entidade e aceite da área cliente.

3.7.2 Planos de Continuidade Operacional devem ser desenvolvidos pelas áreas de negócio do órgão ou entidade para garantir a continuidade dos processos envolvidos nas implantações de software ou outras mudanças relacionadas.

3.7.3 A implantação de novo software deve ser realizada de acordo com o calendário definido pelas áreas de negócio do órgão ou entidade, com a participação da respectiva área de tecnologia da informação.

4. Competências

4.1 Área de Tecnologia da Informação

4.1.1 homologar os procedimentos e metodologias de desenvolvimento externo;

4.1.2 definir treinamentos necessários para os desenvolvedores;

4.1.3 analisar os impactos das solicitações de desenvolvimento e modificações e autorizar ou realizar o desenvolvimento ou a manutenção;

4.1.4 definir procedimentos de testes e implantação de software;

4.1.5 realizar testes no software desenvolvido ou modificado;

4.1.6 homologar software e ferramentas de desenvolvimento de software;

4.1.7 disponibilizar ferramenta para atualizar software no ambiente de produção.

4.2 Áreas de Negócio do Órgão ou Entidade

4.2.1 autorizar a utilização de dados de produção no ambiente de testes;

4.2.2 elaborar procedimentos de homologação, homologar e dar aceite aos produtos desenvolvidos pela área de tecnologia da informação do órgão ou entidade;

4.2.3 elaborar Planos de Continuidade Operacional para garantir a continuidade dos processos envolvidos nas implantações de software ou outras mudanças relacionadas.

5. Documentação Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- ISO/IEC 15408 *Common Criteria - Evaluation Criteria for Information Technology Security*;
- *Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012;*
- Norma 02 - Classificação da de Informação;
- Norma 06 - Contabilização de Ativos de Tecnologia da Informação;
- Norma 07 - Intercâmbio de Informações.

6. Data de Revisão

- 20/09/2013.

Norma 10 – Proteção Contra Código Malicioso

1 Objetivo

Estabelecer diretrizes para a proteção dos recursos de Tecnologia da Informação do IF Baiano contra ação de código malicioso, programas impróprios e acesso não autorizado.

2 Definições

Código Malicioso: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como vírus, cavalo de tróia, spyware, worms, entre outros;

Firewall: sistema de segurança de computadores usado para restringir acesso de/para uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas;

Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (debugging);

Programas Impróprios: programas utilitários utilizados para explorar vulnerabilidades ou burlar a segurança dos recursos de Tecnologia da Informação;

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que utiliza os recursos de Tecnologia da Informação disponibilizados pelo IF Baiano em local ou jornada de trabalho para este último.

3 Diretrizes

3.1 Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de Correio Eletrônico e firewall;

3.2 Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado;

3.3 As atualizações e as correções para os sistemas de detecção e bloqueio de programas maliciosos devem ser homologadas antes de aplicadas ao ambiente de produção;

3.4 É obrigatório o uso de sistemas de detecção e bloqueio de códigos maliciosos em todos os recursos de Tecnologia da Informação;

3.5 Arquivos ou mídias que são utilizados nos equipamentos computacionais devem ser verificados automaticamente, quanto à contaminação por código malicioso, antes de sua utilização;

3.6 Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso;

3.7 Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados pelo *software* antivírus, isolados ou removidos do sistema. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o ambiente de produção;

3.8 Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela área de tecnologia da informação do órgão ou entidade;

3.9 Somente mídias magnéticas e produtos de origem confiável devem ser utilizados nos equipamentos computacionais.

4 Competências

4.1 Área de Tecnologia da Informação

4.1.1 auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;

4.1.2 garantir a instalação dos sistemas de detecção e bloqueio de programas maliciosos nos equipamentos computacionais, mantendo-os atualizados, conforme disponibilização do fabricante;

4.1.3 monitorar os logs dos sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, com objetivo de atuar de forma proativa na identificação de ameaças.

4.2 Usuário

4.2.1 utilizar somente programas homologados;

4.2.2 observar se o programa de antivírus está instalado, atualizado e ativo no equipamento computacional.

5 Documentos Relacionados

- NBR ISO / IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;
- Norma de Segurança da Informação versão 2.0. Secretaria de Administração da Bahia (SAEB), 2012.

6 Data de Revisão

- 20/09/2013.

Publique-se e Cumpra-se

SEBASTIÃO EDSON MOURA

Reitor