NORMA TÉCNICA
ATI-SGR-PR/001.1:09

Norma para Desenvolvimento Seguro de Aplicações Web

Versão 1.0

Válida a partir da publicação da Resolução 001/2009

Palavras-chave: Segurança, Desenvolvimento, Aplicações Web, Sistema.

Ati
Agência Estadual de Tecnologia da Informação

21 páginas

Sumário

Prefácio..... 5
1 Escopo..... 7
2 Termos e definições..... 7
3 Normas..... 10
3.1 Disposições Gerais..... 10
3.2 Validação dos dados..... 10
3.3 Política de senhas..... 11
3.4 Exibição de dados desnecessários..... 11
3.5 Privilégio mínimo..... 12
3.6 Criptografia..... 13
3.7 Upload de arquivos..... 14
3.8 Sistema de autenticação..... 15
3.9 Outras considerações..... 16
4 Verificação de Conformidade..... 17
5 Penalidades..... 17
5.1 Disposições Gerais..... 17
5.2 Comunicação de descumprimento..... 17
5.3 Advertência ou Suspensão..... 18
5.4 Demissão por justa causa..... 18
5.5 Disposições finais..... 19
6 Bibliografia..... 21

Prefácio

A ATI – Agência Estadual de Tecnologia da Informação – é o órgão de coordenação e suporte técnico ao Sistema Estadual de Informática do Governo – SEIG – e que tem como atribuições propor e prover soluções integradoras de meios, métodos e competências, com uso intensivo e adequado da Tecnologia da Informação e Comunicação.

Esta Norma foi elaborada pela Unidade de Segurança da Informação – USI – da ATI com o apoio da Unidade de Sistema de Governo – USG, redigida em conformidade com as convenções redacionais estabelecidas pela ATI e segundo os padrões nacionais e internacionais atualmente utilizados 6.1.1.1.1[1] 6.1.1.1.1[2] 6.1.1.1.1[3] [4].

Esta Norma é parte integrante da Política de Segurança da Informação da ATI 6.1.1.1.1[5], podendo vir a ser substituída ou conviver junto às demais normas de segurança futuramente elaboradas.

Esta Norma foi aprovada pela Diretoria-Executiva de Tecnologia da Informação e Comunicação da ATI (DTI) e entra em vigor na data da publicação da Resolução 005/2009.

1 Escopo

Esta Norma aborda os aspectos de segurança das aplicações Web hospedadas na infraestrutura de *Data Center* da ATI e visa ao estabelecimento de regras para garantir maior segurança para essas aplicações, para os clientes desses serviços e para a ATI, de forma a preservar o ambiente tecnológico no que se refere aos setores computacionais e de comunicação, assim como, prevenir possíveis incidentes de segurança com os dados das aplicações ou com a infraestrutura utilizada.

As regras estabelecidas nesta Norma estendem-se a todos os sistemas aplicativos que estão ou estarão hospedados na ATI, independente de quem os tenha desenvolvido.

Este documento tem como público-alvo: desenvolvedores, programadores, engenheiros de software, arquitetos de software, analistas de suporte, gerentes de projeto e outros atores que sejam, direto ou indiretamente, responsáveis pela construção ou manutenção de aplicações Web hospedadas na ATI.

2 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições:

1

autoridade certificadora

entidade pública ou privada, que estabelece previamente a identidade do futuro portador do certificado digital (pessoa física ou jurídica), por meio dos documentos necessários. Esta entidade também é responsável por emitir esse certificado

2

back-end

termo utilizado para identificar a área do sistema que realizará o processamento das informações repassadas pelo usuário pela interface da aplicação

3

backup

é a cópia de dados de um dispositivo para outro com o objetivo de posteriormente recuperá-los em caso de perda ou dano dos dados originais

4

CAPTCHA – *Completely Automated Public Turing test to tell Computers and Humans Apart*

técnica de verificação que uma requisição parte de uma pessoa e não de um *script*. Essa técnica é conhecida pelo uso de uma imagem com um texto, onde o usuário informará para a aplicação os caracteres que aparecem nessa imagem.

5

certificado auto-assinado

tipo de certificado digital emitido por pessoas ou organizações que não possuem autorização da Infraestrutura de Chaves Públicas (ICP). Desse modo, esses certificados são ditos inválidos, pois não transmitem confiança alguma. Apesar disso, esses certificados garantem a criptografia do tráfego, mas não garantem a identificação do servidor

6

debug

processo de localização e remoção de erros nas aplicações por meio de mensagens de erros disponibilizadas pelo sistema

7

função hash

função que recebe dados de comprimento arbitrário, comprime estes dados e devolve um número fixo de bits, o resultado *hash*. Para que a função possa ser utilizada em aplicações criptográficas, ela deverá ter a propriedade que garante que seja impossível ou impraticável encontrar pares de mensagens que gerem resultados *hash* iguais

8

log

arquivo onde são armazenados eventos à medida que esses ocorrem. Utilizado em auditorias para diagnosticar problemas etc.

9

SGBD

Sistema Gerenciador de Banco de Dados (comum no Brasil) ou Sistema Gestor de Base de Dados, é um conjunto de programas de computador (softwares) responsáveis pelo gerenciamento de uma base de dados

10

upload

é o envio de dados ou arquivos, pela rede, de um computador para outro

3 Normas

3.1 Disposições Gerais

As normas abaixo relacionadas trazem como premissa básica o conceito de que tudo o que não for permitido e/ou liberado é considerado violação à Política de Segurança da Informação da ATI [5].

Salienta-se que, em virtude de ser a segurança da informação um processo contínuo e de estar a ATI em pleno processo de elaboração e implantação de sua Política de Segurança da Informação, novas normas e possíveis alterações de versão estarão sendo implementadas. Neste último caso, revogando-se, automaticamente, a norma anterior, devendo, portanto, todos os responsáveis pelo desenvolvimento ou manutenção de sistemas aplicativos a serem hospedados no ambiente da ATI, manterem-se atualizados e obedientes às normas em vigor que serão disponibilizadas pela ATI para fins de conhecimento.

3.2 Validação dos dados

A seguir, é descrita a ação a ser adotada pela aplicação para a validação dos campos de entrada de dados:

a) todos os dados de entrada deverão ser validados pela aplicação. Esta validação deverá ocorrer, pelo menos, no lado do servidor (*back-end*, ver 2.1.1.1.1[1]2). Por exemplo, campos numéricos deverão ter apenas números, campos de data deverão ter apenas números e caracteres separadores e deverão estar num formato de data.

3.3 Política de senhas

A seguir são descritas as ações a serem adotadas pela aplicação para garantir que os usuários utilizem senhas fortes:

a) a aplicação deverá possuir uma política de senhas, obrigando a seus usuários utilizarem senhas fortes 6.1.1.1.1[6].

b) a senha do usuário deverá ser trocada periodicamente, no máximo a cada 90 dias. Para isso, a aplicação deverá ter um controle sobre a data de modificação da senha e obrigar ao usuário trocá-la, no caso da expiração do prazo. Além disso, a aplicação deverá manter um histórico, com no mínimo 1 (uma) senha, impedindo que o usuário a reutilize como sua senha atual.

3.4 Exibição de dados desnecessários

Os itens a seguir apresentam algumas ações que podem ser adotadas pela aplicação para evitar que sejam divulgadas informações, as quais permitam ou facilitem a ação de um atacante.

a) a fim de impedir a visualização de arquivos indevidamente acessíveis via web, tais como arquivos temporários, arquivos de *backup* (ver 2.1.1.1.1[1]3) e arquivos de *log* (ver 2.1.1.1.1[1]8), torna-se necessário que esses arquivos não sejam disponibilizados na estrutura da aplicação Web. Essa medida é necessária, pois os arquivos podem conter informações que possibilitem maior conhecimento da aplicação, tal como a visualização do código-fonte ou mesmo, o acesso a dados confidenciais, tais como *login* e senha da base de dados. Além disso, os arquivos compactados, quando

utilizados como *backup* de outros arquivos ou do próprio site, também deverão ser removidos da aplicação;

b) toda aplicação deverá ser configurada para evitar a listagem de seus diretórios, evitando assim, que um atacante tenha conhecimento da sua estrutura de arquivos e pastas;

c) a aplicação deverá ser configurada e desenvolvida para que não exiba mensagens de erro detalhadas, tais como mensagens de *debug* (ver 2.1.1.1.1[1]6). Ao invés disso, o desenvolvedor poderá armazenar ou repassar internamente as mensagens. Estas mensagens podem ajudar a descobrir informações tais como o SGBD (ver 2.1.1.1.1[1]9) utilizado, versão do serviço utilizado, nomes de campos e tabelas do banco de dados, caminho físico dos arquivos no servidor etc. As mensagens de erro devem conter informações mínimas que ajudem o usuário no problema, mas que não forneçam informações desnecessárias;

d) comentários com informações sensíveis, disponibilizadas no código HTML gerado, deverão ser suprimidos.

3.5 Privilégio mínimo

As ações descritas a seguir devem ser adotadas pela aplicação a fim de evitar a disponibilidade de permissões desnecessariamente.

a) o servidor deverá ser configurado para executar somente os serviços necessários aos sistemas presentes. Removendo ou desabilitando quaisquer outros serviços que não sejam necessários para suas finalidades;

b) os usuários dos serviços oferecidos pela aplicação deverão possuir o mínimo de privilégio possível, a fim de evitar acessos indevidos à aplicação, o que pode afetar o ambiente que a hospeda. Essa medida deverá ser ampliada para os usuários utilizados numa possível conexão com a base de dados. Desse modo, caso a aplicação realize somente consultas na base de dados, apenas a permissão de leitura para a base específica deverá ser disponibilizada. Em nenhuma hipótese há a necessidade de se utilizar um usuário administrador da base de dados;

c) esse conceito de privilégio mínimo deverá também ser utilizado internamente para os usuários da aplicação, disponibilizando para estes somente as permissões necessárias para a realização do seu trabalho.

3.6 Criptografia

As ações a seguir devem ser adotadas pela aplicação, caso essa contenha informações sigilosas ou algum sistema de autenticação.

a) caso a aplicação contenha dados confidenciais, recomenda-se a utilização de um certificado digital a fim de garantir a confidencialidade dos dados. O certificado poderá ser auto-assinado (ver 2.1.1.1.1[1]5), caso a aplicação seja utilizada na Intranet. De outra forma, caso esteja disponível para a Internet, recomenda-se ser assinado por uma autoridade certificadora (ver 2.1.1.1.1[1]1);

b) as informações confidenciais armazenadas na base de dados deverão ser criptografadas utilizando-se algoritmos de criptografia públicos, amplamente utilizados e recomendados por instituições especializadas. Dados tais como senhas, devem ser armazenados utilizando-se funções

hash (ver 2.1.1.1.1[1]7). Devido à rápida evolução de técnicas capazes de quebrar esses algoritmos, este documento não apresenta exemplos de soluções a serem utilizados na aplicação. Para mais informações sobre quais algoritmos poderão ser utilizados, consultar a Unidade de Segurança da Informação – USI, por intermédio da Gerência de Relacionamento do Governo – GRG – da ATI.

3.7 Upload de arquivos

Para as aplicações que disponibilizam alguma funcionalidade de *upload* (ver 2.1.1.1.1[1]10) as seguintes ações são recomendadas:

a) a aplicação deverá realizar uma restrição dos formatos de arquivos aceitos para o *upload*. A restrição deverá ser baseada numa lista de extensões de arquivos previamente definidos, impedindo desse modo, que quaisquer outros formatos que não estejam nesta listagem sejam permitidos. Algumas extensões que podem ser utilizadas são as de documentos, imagens, vídeos etc. As extensões que devem ser proibidas são as executáveis, as de *script*, código-fonte, de arquivos compactados etc;

b) deve haver uma limitação do tamanho dos arquivos enviados, assim como, da quantidade de arquivos enviados por cada usuário dentro de um intervalo de tempo. Estes requisitos visam prevenir que a aplicação sofra um ataque de negação de serviços, como o que acontece nos casos em que algum usuário envie muitos arquivos pequenos ou poucos arquivos grandes, evitando com isso, que o espaço em disco seja esgotado. O ataque de negação de serviços para esta finalidade tem como efeito mínimo o de impossibilitar que novos arquivos sejam inseridos e, o efeito

máximo de travamento do servidor. Este último ocorrerá, pois nem mesmo o sistema operacional poderá escrever na partição, caso o *upload* esteja sendo realizado na mesma partição do sistema operacional;

c) deverá existir uma partição exclusiva para o *upload* de arquivos. A intenção é evitar que o sistema operacional seja afetado pela falta de espaço livre na partição;

d) não deverá ser exibida para o usuário a opção de escolha do local de armazenamento de cada arquivo enviado. Com isso, a intenção é impedir que o usuário tome conhecimento da estrutura de arquivos e diretórios ou até mesmo que ele envie arquivos para áreas proibidas, por exemplo, áreas do sistema operacional ou mesmo dos arquivos da aplicação;

e) deverá haver um gerenciamento nos nomes dos arquivos enviados, prevenindo que arquivos já existentes sejam sobrescritos. Isso evita que o usuário sobrescreva arquivos de outros usuários ou até mesmo da aplicação.

3.8 Sistema de autenticação

A seguir são apresentadas as ações a serem adotadas pela aplicação para aumentar a segurança na autenticação dos usuários, a fim de evitar que acessos indevidos ocorram.

a) qualquer recurso protegido só deverá ser acessado por um usuário devidamente autenticado e com as permissões necessárias para acessá-lo;

b) a fim de evitar ataques ao sistema de autenticação, tais como os ataques

de força bruta, a aplicação deverá utilizar CAPTCHA (ver 2.1.1.1.1[1]4) logo após a primeira falha na autenticação. Além disso, após a 5º tentativa de *logon* sem sucesso, o sistema deverá bloquear a conta do usuário por 15 minutos;

c) caso a aplicação possua uma área administrativa, essa deverá, sempre que possível, ter o acesso restrito para o IP do órgão/secretaria e/ou fornecedor. Com isso, evita-se que o serviço seja desnecessariamente acessado por pessoas não autorizadas.

3.9 Outras considerações

a) todas as atualizações de segurança relativas ao sistema operacional deverão ser instaladas no servidor;

b) todos os serviços utilizados no servidor deverão ser atualizados, caso novas versões sejam disponibilizadas com correções de segurança. Por outro lado, caso a atualização apresente apenas novas funcionalidades ou correções de falhas que não tratem de problemas de segurança, fica a cargo do responsável por manter a aplicação, decidir pela instalação da atualização;

c) o administrador do servidor deverá configurar cada serviço, a fim de aumentar a segurança. Como cada serviço possui suas peculiaridades, recomenda-se consultar a documentação do desenvolvedor, verificando as configurações a serem realizadas na instalação e manutenção do sistema aplicativo.

4 Verificação de Conformidade

Para garantir o cumprimento das regras anteriormente mencionadas, a ATI deverá utilizar o seguinte meio:

a) auditoria das aplicações hospedadas no ambiente da ATI pela equipe técnica da Unidade de Segurança da Informação – USI – em conjunto com a Unidade de Data Center – UDC, para monitoração de itens em desconformidade com as prescrições estabelecidas por esta Norma.

5 Penalidades

5.1 Disposições Gerais

O não cumprimento das normas estabelecidas neste documento (Norma para Desenvolvimento Seguro de Aplicações Web), por funcionário da ATI, órgão, secretaria ou fornecedor, seja isolada ou cumulativamente, poderá implicar, de acordo com a infração cometida, em punições conforme descritas nas seções a seguir, além das previstas em outros instrumentos normativos.

5.2 Comunicação de descumprimento

a) será encaminhada ao responsável uma notificação informando o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada também, uma cópia para o seu superior imediato;

b) o serviço que estiver em desacordo com este instrumento, será desativado até que a(s) falha(s) seja(m) corrigida(s) pelo seu responsável.

5.3 Advertência ou Suspensão

a) a pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação, no caso de funcionários da ATI, por meio de processo administrativo disciplinar.

5.4 Demissão por justa causa

a) a pena de demissão por justa causa será aplicada nos casos legais e após regular apreciação, no caso de funcionários da ATI, por meio de processo administrativo disciplinar;

b) aos funcionários enquadrados no regime de trabalho CLT (Consolidação das Leis do Trabalho), ditos “empregados”, a pena de demissão por justa causa será aplicada nas hipóteses previstas no art. 482, Parágrafo único, da Consolidação das Leis do Trabalho, Decreto-lei nº 5.452, de 1º de maio de 1943;

c) aos funcionários enquadrados no regime de trabalho ESTATUTÁRIO, ditos “servidores públicos”, a pena de demissão será aplicada nas hipóteses previstas no art. 204, da Lei 6.123, de 20 de julho de 1968, do Estatuto dos Funcionários Públicos do Estado de Pernambuco, e nas hipóteses das penas pelo cometimento de crime contra a administração pública previstas no Decreto-Lei n° 2.848, de 7 de dezembro de 1940, do Código Penal;

d) aos funcionários sob cargo em comissão, a pena de exoneração será aplicada com base no art. 37, inciso II, da Constituição Federal, nas

hipóteses previstas no art. 204, da Lei 6.123, de 20 de julho de 1968, do Estatuto dos Funcionários Públicos do Estado de Pernambuco, e nas hipóteses das penas pelo cometimento de crime contra a administração pública previstas no Decreto-Lei n° 2.848, de 7 de dezembro de 1940, do Código Penal;

e) aos funcionários terceirizados e prestadores de serviço, será solicitado à empresa prestadora da respectiva mão-de-obra, o afastamento definitivo do funcionário, podendo a ATI solicitar a substituição deste ou até mesmo, rescindir o contrato de prestação de serviço, conforme cláusulas contratuais pré-estabelecidas.

5.5 Disposições finais

Salienta-se que as medidas punitivas das seções 5.3 e 5.4 deste instrumento terão impacto sobre os funcionários da ATI, tanto sob o regime do estatuto, como sob o regime da CLT. Para os demais casos, aplica-se inicialmente o disposto na seção 5.2, salvo disposição em instrumento normativo específico.

6 Bibliografia

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBRISO/IEC27001, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos, mar. de 2006.

[2] ABNT. NBRISO/IEC27002, Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, ago. de 2005.

[3] ABNT. NBRISO/IEC27005, Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação, jul. de 2006.

[4] ATI – Agência Estadual de Tecnologia da Informação. Norma para elaboração, estruturação e redação de normas técnicas para o SEIG. Versão 1.0 – Recife, 2009.

[5] ATI. Comitê Gestor de Segurança. Política de Segurança da Informação. Resolução 001/2008, de 13 de maio de 2008. Versão 1.0 – Recife, 2008. Disponível em: <www.ati.pe.gov.br>. Acesso em: 12 de jan. de 2009.

[6] ATI. Recomendações de Uso e Formação de Senhas. Recife, 2008. Disponível em: <http://www2.ati.pe.gov.br/web/siteati/recomendacoes2>. Acesso em: 16 de jan. de 2009.