

TRIBUNAL DE CONTAS DA UNIÃO

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO





TRIBUNAL DE CONTAS DA UNIÃO
Secretaria-Geral de Controle Externo
Secretaria Adjunta de Fiscalização

**BOAS PRÁTICAS EM
SEGURANÇA DA
INFORMAÇÃO**

Diretoria de Auditoria da Tecnologia da Informação

Brasília, 2003

Brasil. Tribunal de Contas da União.

Boas práticas em segurança da informação / Tribunal de Contas da União. – Brasília : TCU, Secretaria Adjunta de Fiscalização, 2003.

70p.

1. Segurança da informação 2. Auditoria, Tecnologia da informação I. Título.



TRIBUNAL DE CONTAS DA UNIÃO

Negócio: Controle Externo da Administração Pública e da gestão dos recursos públicos federais

Missão: Assegurar a efetiva e regular gestão dos recursos públicos, em benefício da sociedade

Visão: Ser instituição de excelência no controle e contribuir para o aperfeiçoamento da Administração Pública

MINISTROS

Valmir Campelo, Presidente
Adylson Motta, Vice-Presidente
Marcos Vinícios Rodrigues Vilaça
Iram Saraiva
Humberto Souto
Walton Alencar Rodrigues
Guilherme Palmeira
Ubiratan Aguiar
Benjamin Zymler

MINISTROS-SUBSTITUTOS

Lincoln Magalhães da Rocha
Augusto Sherman Cavalcanti
Marcos Bemquerer Costa

MINISTÉRIO PÚBLICO

Lucas Rocha Furtado, Procurador-Geral
Jatir Batista da Cunha, Subprocurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Ubaldo Alves Caldas, Subprocurador-Geral
Maria Alzira Ferreira, Procuradora
Marinus Eduardo Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora

Apresentação

É notória a dependência das organizações atuais aos sistemas informatizados. Cresce a quantidade e a complexidade de sistemas computacionais que controlam os mais variados tipos de operações e o próprio fluxo de informações das organizações. Com efeito, a Administração Pública brasileira, reflexo da própria sociedade em geral, está cada vez mais adotando o computador como ferramenta indissociável na busca da excelência na produção de bens e na prestação de serviços.

A informatização crescente reclama especial atenção das organizações, uma vez que a utilização da tecnologia da informação para a manipulação e armazenamento de dados introduz novos riscos e aumenta a fragilidade de algumas atividades. Assim, torna-se imperativa a atenção de todos os gestores públicos para as questões relacionadas à segurança da tecnologia da informação.

Grande parte dos órgãos e entidades sob a jurisdição do TCU já utiliza maciçamente a tecnologia da informação para automatizar sua operação e registrar, processar, manter e apresentar informações. Com o intuito de incrementar e aperfeiçoar as atividades de auditoria desenvolvidas pelo corpo técnico do Tribunal, enfrentando a dificuldade de exercer o controle externo de entidades informatizadas, aprovei a criação do Projeto da Auditoria da Tecnologia da Informação em fevereiro deste ano. Os objetivos desse Projeto são: pesquisar, desenvolver e disseminar ferramentas, técnicas e documentos para apoiar a Auditoria da Tecnologia da Informação, bem como, manter um núcleo especializado para apoiar os auditores do Tribunal e disseminar as “boas práticas” em tecnologia da informação para os fiscalizados.

O Tribunal de Contas da União, ciente da importância de seu papel pedagógico junto aos administradores públicos e da utilidade de apresentar sua forma de atuação às unidades jurisdicionadas e prefeituras, elaborou esta publicação com intuito de despertar a atenção para os aspectos da segurança da tecnologia da informação nas organizações governamentais. Espera-se que esse trabalho seja uma boa fonte de consulta e que o Tribunal, mais uma vez, colabore para o aperfeiçoamento da Administração Pública.

Valmir Campelo

Presidente

Sumário

Introdução	9
Controles de Acesso Lógico	11
Política de Segurança de Informações	27
Plano de Contingências	35
Anexos	41

Introdução

Na sociedade da informação, ao mesmo tempo que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança de informações tornou-se um ponto crucial para a sobrevivência das instituições.

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

O objetivo desta publicação é apresentar, na forma de capítulos, boas práticas em segurança da informação, a qualquer pessoa que interaja de alguma forma com ambientes informatizados, desde profissionais de informática envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e os negócios de sua organização, em especial, os gestores da Administração Pública Federal. Esta primeira publicação conta com três capítulos: controles de acesso lógico, política de segurança de informações e plano de contingências. É nossa intenção publicar novas edições, incluindo capítulos sobre assuntos correlatos, como controles organizacionais, controles sobre bancos de dados, ambiente cliente/servidor, entre outros.

1. Controles de Acesso Lógico

Neste capítulo serão apresentados conceitos importantes sobre controles de acesso lógico a serem implantados em instituições que utilizam a informática como meio de geração, armazenamento e divulgação de informações, com o objetivo de prover segurança de acesso a essas informações.

1.1. O que são controles de acesso?

Os controles de acesso, físicos ou lógicos, têm como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Os sistemas computacionais, bem diferentes de outros tipos de recursos, não podem ser facilmente controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardas de segurança.

1.2. O que são controles de acesso lógico?

Os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo

de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas de computador.

O controle de acesso lógico pode ser encarado de duas formas diferentes : a partir do recurso computacional que se quer proteger e a partir do usuário a quem serão concedidos certos privilégios e acessos aos recursos.

A proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário, enquanto que a identificação e autenticação do usuário (confirmação de que o usuário realmente é quem ele diz ser) é feita normalmente através de um identificador de usuário (ID) e uma senha durante o processo de logon no sistema.

1.3. Que recursos devem ser protegidos?

A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

Abaixo serão apresentados os motivos pelos quais esses recursos devem ser protegidos.

- Aplicativos (programas fonte e objeto)

O acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa. Por exemplo, em um aplicativo bancário, pode-se zerar os centavos de todas as contas correntes e transferir o total dos centavos para uma determinada conta, beneficiando ilegalmente esse correntista.

- Arquivos de dados

Bases de dados, arquivos ou transações de bancos de dados devem ser protegidos para evitar que os dados sejam apagados ou alterados sem autorização, como por exemplo, arquivos com a configuração do sistema, dados da folha de pagamento, dados estratégicos da empresa.

- Utilitários e sistema operacional

O acesso a utilitários, como editores, compiladores, softwares de manutenção, monitoração e diagnóstico deve ser restrito, já que essas ferramentas podem ser usadas para alterar aplicativos, arquivos de dados e de configuração do sistema operacional, por exemplo.

O sistema operacional é sempre um alvo bastante visado, pois sua configuração é o ponto chave de todo o esquema de segurança. A fragilidade do sistema operacional compromete a segurança de todo o conjunto de aplicativos, utilitários e arquivos.

- Arquivos de senha

A falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter identificador (ID) e senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema. Essa pessoa dificilmente será barrada por qualquer controle de segurança instalado, já que se faz passar por um usuário autorizado.

- Arquivos de log

Os arquivos de log são usados para registrar ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras. Os logs registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas.

Um invasor ou usuário não autorizado pode tentar acessar o sistema, apagar ou alterar dados, acessar aplicativos, alterar a configuração do sistema operacional para facilitar futuras invasões e depois alterar os arquivos de log para que suas ações não possam ser identificadas. Dessa forma, o administrador do sistema não ficará sabendo que houve uma invasão.

1.4. O que os controles de acesso lógico pretendem garantir em relação à segurança de informações?

Os controles de acesso lógico são implantados com o objetivo de garantir que:

- apenas usuários autorizados tenham acesso aos recursos;

- os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas tarefas;

- o acesso a recursos críticos seja bem monitorado e restrito a poucas pessoas;

- os usuários estejam impedidos de executar transações incompatíveis com sua função ou além de suas responsabilidades.

O controle de acesso pode ser traduzido, então, em termos de funções de identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos; e prevenção de acessos não autorizados.

1.5. Como os usuários são identificados e autenticados?

Os usuários dos sistemas computacionais são identificados e autenticados durante um processo, chamado Logon. Os processos de logon são usados para conceder acesso aos dados e aplicativos em um sistema computacional e orientam os usuários durante sua identificação e autenticação.

Normalmente esse processo envolve a entrada de um ID (identificação do usuário) e uma senha (autenticação do usuário). A identificação define para o computador quem é o usuário e a

senha é um autenticador, isto é, ela prova ao computador que o usuário é realmente quem ele diz ser.

1.5.1. Como deve ser projetado um processo de logon para ser considerado eficiente?

O procedimento de logon deve divulgar o mínimo de informações sobre o sistema, evitando fornecer, a um usuário não autorizado, informações detalhadas. Um procedimento de logon eficiente deve:

- informar que o computador só deve ser acessado por pessoas autorizadas;

- evitar identificar o sistema ou suas aplicações até que o processo de logon esteja completamente concluído;

- durante o processo de logon, evitar o fornecimento de mensagens de ajuda que poderiam auxiliar um usuário não autorizado a completar esse procedimento;

- validar a informação de logon apenas quando todos os dados de entrada estiverem completos. Caso ocorra algum erro, o sistema não deve indicar qual parte do dado de entrada está correta ou incorreta, como por exemplo, ID ou senha;

- limitar o número de tentativas de logon sem sucesso (é recomendado um máximo de três tentativas), e ainda:

- a) registrar as tentativas de acesso inválidas;

b) forçar um tempo de espera antes de permitir novas tentativas de entrada no sistema ou rejeitar qualquer tentativa posterior de acesso sem autorização específica;

c) encerrar as conexões com o computador.

· limitar o tempo máximo para o procedimento de logon. Se excedido, o sistema deverá encerrar o procedimento;

· mostrar as seguintes informações, quando o procedimento de logon no sistema finalizar com êxito:

a) data e hora do último logon com sucesso;

b) detalhes de qualquer tentativa de logon sem sucesso, desde o último procedimento realizado com sucesso.

1.5.2. O que é identificação do usuário?

A identificação do usuário, ou ID, deve ser única, isto é, cada usuário deve ter uma identificação própria. Todos os usuários autorizados devem ter um ID, quer seja um código de caracteres, cartão inteligente ou qualquer outro meio de identificação. Essa unicidade de identificação permite um controle das ações praticadas pelos usuários através dos logs.

No caso de identificação a partir de caracteres, é comum estabelecer certas regras de composição, como por exemplo, quantidade mínima e máxima de caracteres, misturando letras, números e símbolos.

1.5.3 O que é autenticação do usuário?

Após a identificação do usuário, deve-se proceder à sua autenticação, isto é, o sistema deve confirmar se o usuário é realmente quem ele diz ser. Os sistemas de autenticação são uma combinação de hardware, software e procedimentos que permitem o acesso de usuários aos recursos computacionais.

Na autenticação, o usuário deve apresentar algo que só ele saiba ou possua, podendo até envolver a verificação de características físicas pessoais. A maioria dos sistemas atuais solicita uma senha (algo que, supostamente, só o usuário conhece), mas já existem sistemas mais modernos utilizando cartões inteligentes (algo que o usuário possui) ou ainda características físicas (algo intrínseco ao usuário), como o formato da mão, da retina ou do rosto, impressão digital e reconhecimento de voz.

1.5.4. Como orientar os usuários em relação às senhas?

Para que os controles de senha funcionem, os usuários devem ter pleno conhecimento das políticas de senha da organização e devem ser orientados e estimulados a segui-las fielmente. Todos os usuários devem ser solicitados a:

· manter a confidencialidade das senhas;

· não compartilhar senhas;

· evitar registrar as senhas em papel;

- selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que os obriguem a escrevê-las em um pedaço de papel para não serem esquecidas (recomenda-se tamanho entre seis e oito caracteres);

- alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

- alterar a senha em intervalos regulares ou com base no número de acessos (senhas para usuários privilegiados devem ser alteradas com maior frequência que senhas normais);

- evitar reutilizar as mesmas senhas;

- alterar senhas temporárias no primeiro acesso ao sistema;

- não incluir senhas em processos automáticos de acesso ao sistema (por exemplo, armazenadas em macros).

Vale lembrar também que utilizar a mesma senha para vários sistemas não é uma boa prática, pois a primeira atitude de um invasor, quando descobre a senha de um usuário em um sistema vulnerável, é tentar a mesma senha em outros sistemas a que o usuário tem acesso.

1.5.5. Que tipos de senhas devem ser evitadas?

Os usuários devem evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo :

- nome do usuário;

- identificador do usuário (ID), mesmo que seus caracteres estejam embaralhados;

- nome de membros de sua família ou de amigos íntimos;

- nomes de pessoas ou lugares em geral;

- nome do sistema operacional ou da máquina que está sendo utilizada;

- nomes próprios;

- datas;

- números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;

- placas ou marcas de carro;

- palavras que constam de dicionários em qualquer idioma;

- letras ou números repetidos;

- letras seguidas do teclado do computador (ASDFG, YUIOP);

- objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela);

- qualquer senha com menos de 6 caracteres.

Alguns softwares são capazes de identificar senhas frágeis, como algumas dessas citadas acima, a partir de bases de dados de nomes e seqüências de caracteres mais comuns, e ainda bloquear a escolha dessas senhas por parte do usuário. Essas bases de dados normalmente fazem parte do pacote de software de segurança e podem ser atualizadas pelo gerente de segurança com novas inclusões.

1.5.6. Como escolher uma boa senha?

Geralmente são consideradas boas senhas aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando mais de seis caracteres. Porém, para ser boa mesmo, a senha tem que ser difícil de ser adivinhada por outra pessoa, mas de fácil memorização, para que não seja necessário anotá-la em algum lugar. Também é conveniente escolher senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a uma certa distância ou por cima de seus ombros, possam identificar a seqüência de caracteres.

Um método bastante difundido hoje em dia é selecionar uma frase significativa para o usuário e utilizar os primeiros caracteres de cada palavra que a compõe, inserindo símbolos entre eles. É também recomendável não utilizar a mesma senha para vários sistemas. Se um deles não for devidamente protegido, a senha poderá ser descoberta e utilizada nos sistemas que, a priori, estariam seguros. Outro conselho : adquira o hábito de trocar sua senha com freqüência. Trocá-la a cada 60/90 dias é considerado uma boa prática.

Se você realmente não conseguir memorizar sua senha e tiver que escrevê-la em algum pedaço de papel, tenha pelo menos o cuidado de não identificá-la como sendo uma senha. Não pregue esse pedaço de papel no próprio computador, não guarde a senha junto com a sua identificação de usuário e nunca a envie por e-mail ou armazene em arquivos do computador.

1.5.7. Como deve ser feita a concessão de senhas aos usuários?

A concessão de senhas deve ser feita de maneira formal, considerando os seguintes pontos:

- solicitar aos usuários a assinatura de uma declaração, a fim de manter a confidencialidade de sua senha pessoal (isso pode estar incluso nos termos e condições do contrato de trabalho do usuário);
- garantir, aos usuários, que estão sendo fornecidas senhas iniciais seguras e temporárias, forçando-os a alterá-las logo no primeiro login. O fornecimento de senhas temporárias, nos casos de esquecimento por parte dos usuários, deve ser efetuado somente após a identificação positiva do respectivo usuário;
- fornecer as senhas temporárias aos usuários de forma segura. O uso de terceiros ou mensagens de correio eletrônico desprotegidas (não criptografadas) deve ser evitado.

1.5.8. O que a instituição pode fazer para proteger e controlar as senhas de acesso a seus sistemas?

O sistema de controle de senhas deve ser configurado para proteger as senhas armazenadas contra uso não autorizado, sem apresentá-las na tela do computador, mantendo-as em arquivos cripto-grafados e estipulando datas de expiração (normalmente se recomenda a troca de senhas após 60 ou 90 dias). Alguns sistemas, além de criptografar as senhas, ainda guardam essas informações em arquivos escondidos que não podem ser vistos por usuários, dificultando, assim, a ação dos hackers.

Para evitar o uso freqüente das mesmas senhas, o sistema de controle de senhas deve manter um histórico das últimas senhas utilizadas por cada usuário. Deve-se ressaltar, entretanto, que a troca muito freqüente de senhas também pode confundir o usuário, que poderá passar a escrever a senha em algum lugar visível ou escolher uma senha mais fácil, comprometendo, assim, sua segurança.

O gerente de segurança deve desabilitar contas inativas, sem senhas ou com senhas padronizadas. Até mesmo a senha temporária fornecida ao usuário pela gerência de segurança deve ser gerada de forma que já entre expirada no sistema, exigindo uma nova senha para os próximos logons. Portanto, deve haver um procedimento que force a troca de senha imediatamente após a primeira autenticação, quando o usuário poderá escolher a senha que será utilizada dali por diante.

Ex-funcionários devem ter suas senhas bloqueadas. Para isso, devem existir procedimentos administrativos eficientes que informem o gerente de segurança, ou o administrador dos sistemas, da ocorrência de demissões ou desligamentos de fun-

cionários. Esses procedimentos, na prática, nem sempre são seguidos, expondo a organização a riscos indesejáveis.

Também devem ser bloqueadas contas de usuários após um determinado número de tentativas de acesso sem sucesso. Esse procedimento diminui os riscos de alguém tentar adivinhar as senhas. Attingido esse limite, só o administrador do sistema poderá desbloquear a conta do usuário, por exemplo.

1.5.9. Existem outras formas de autenticação do usuário, além do uso de senhas?

Sim. A autenticação dos usuários pode ser feita a partir de tokens, ou ainda, sistemas biométricos.

1.5.10. O que são tokens?

A idéia de fornecer tokens aos usuários como forma de identificá-los é bastante antiga. No nosso dia-a-dia estamos freqüentemente utilizando tokens para acessar alguma coisa. As chaves que abrem a porta da sua residência ou seu cartão com tarja magnética para utilizar o caixa eletrônico do banco são exemplos de tokens. O cartão magnético é ainda uma token especial, pois guarda outras informações, como por exemplo, sua conta bancária.

Token pode ser definida, então, como um objeto que o usuário possui, que o diferencia das outras pessoas e o habilita a acessar algum objeto. A desvantagem das tokens em relação às senhas é que as tokens, por serem objetos, podem ser perdidas, roubadas ou reproduzidas com maior facilidade.

1.5.11. O que são cartões magnéticos inteligentes?

Os cartões inteligentes são tokens que contêm microprocessadores e capacidade de memória suficiente para armazenar dados, a fim de dificultar sua utilização por outras pessoas que não seus proprietários legítimos.

O primeiro cartão inteligente, patenteado em 1975, foi o de Roland Moreno, considerado o pai do cartão inteligente. Comparado ao cartão magnético, que é um simples dispositivo de memória, o cartão inteligente não só pode armazenar informações para serem lidas, mas também é capaz de processar informações. Sua clonagem é mais difícil e a maioria dos cartões inteligentes ainda oferece criptografia.

Normalmente o usuário de cartão inteligente precisa fornecer uma senha à leitora de cartão para que o acesso seja permitido, como uma medida de proteção a mais contra o roubo de cartões.

As instituições bancárias, financeiras e governamentais são os principais usuários dessa tecnologia, em função de seus benefícios em relação à segurança de informações e pela possibilidade de redução de custos de instalações e pessoal, como por exemplo, a substituição dos guichês de atendimento ao público nos bancos por caixas eletrônicos. Os cartões inteligentes têm sido usados em diversas aplicações: cartões bancários, telefônicos e de crédito, dinheiro eletrônico, segurança de acesso, carteiras de identidade.

1.5.12. O que são sistemas biométricos?

Os sistemas biométricos são sistemas automáticos de verificação de identidade baseados em características físicas do usuário. Esses sistemas têm como objetivo suprir deficiências de segurança das senhas, que podem ser reveladas ou descobertas, e das tokens, que podem ser perdidas ou roubadas.

Os sistemas biométricos automáticos são uma evolução natural dos sistemas manuais de reconhecimento amplamente difundidos há muito tempo, como a análise grafológica de assinaturas, a análise de impressões digitais e o reconhecimento de voz. Hoje já existem sistemas ainda mais sofisticados, como os sistemas de análise da conformação dos vasos sanguíneos na retina.

1.5.13. Que características humanas podem ser verificadas por sistemas biométricos?

Teoricamente, qualquer característica humana pode ser usada como base para a identificação biométrica. Na prática, entretanto, existem algumas limitações. A tecnologia deve ser capaz de medir determinada característica de tal forma que o indivíduo seja realmente único, distinguindo inclusive gêmeos, porém não deve ser invasiva ou ferir os direitos dos indivíduos.

Um dos problemas enfrentados pelos sistemas biométricos atuais é sua alta taxa de erro, em função da mudança das características de uma pessoa com o passar dos anos, ou devido a problemas de saúde ou nervosismo, por exemplo.

A tolerância a erros deve ser estabelecida com precisão, de forma a não ser grande o suficiente para admitir impostores, nem pequena demais a ponto de negar acesso a usuários legítimos. Abaixo serão apresentadas algumas características humanas verificadas por sistemas biométricos existentes:

- Impressões digitais – são características únicas e consistentes. Nos sistemas biométricos que utilizam essa opção, são armazenados de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão lida com impressões digitais de pessoas autorizadas, armazenadas em sua base de dados. Atualmente, estão sendo utilizadas impressões digitais em alguns sistemas governamentais, como por exemplo, o sistema de previdência social na Espanha e o de registro de eleitores na Costa Rica;

- Voz – os sistemas de reconhecimento de voz são usados para controle de acesso, porém não são tão confiáveis quanto às impressões digitais, em função dos erros causados por ruídos do ambiente e problemas de garganta ou nas cordas vocais das pessoas a eles submetidas;

- Geometria da mão – também é usada em sistemas de controle de acesso, porém essa característica pode ser alterada por aumento ou diminuição de peso ou artrite;

- Configuração da íris e da retina – os sistemas que utilizam essas características se propõem a efetuar identificação mais confiável do que os sistemas que verificam impressões digitais. Entretanto, são sistemas invasivos, pois direcionam feixes de luz aos olhos das pessoas que se submetem à sua identificação;

- Reconhecimento facial através de termogramas - o termograma facial é uma imagem captada por uma câmera infravermelha que mostra os padrões térmicos de uma face. Essa imagem é única e, combinada com algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se em uma técnica não invasiva, altamente confiável, não sendo afetada por alterações de saúde, idade ou temperatura do corpo. São armazenados ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. O desenvolvimento dessa tecnologia tem como um de seus objetivos baratear seu custo para que possa ser usada em um número maior de aplicações de identificação e autenticação.

1.6. Como restringir o acesso aos recursos informacionais?

O fato de um usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem qualquer restrição. Deve-se implementar um controle específico restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na organização. Esse controle pode ser feito por menus, funções ou arquivos.

1.6.1. Para que servem os controles de menu?

Os controles de menu podem ser usados para restringir o acesso de diferentes categorias de usuários apenas àqueles aplicativos ou utilitários indispensáveis a cada categoria.

Por exemplo, em um sistema de folha de pagamento, poderá ser apresentado um menu inicial com três opções diferentes : funcionário, gerente e setor de recursos humanos. Nesse caso, o administrador do sistema deverá conceder acesso a cada uma das opções de acordo com a função desempenhada pelo usuário. Portanto, o funcionário só terá acesso a dados da sua folha de pagamento pessoal, enquanto que o gerente poderá ter acesso a algumas informações da folha de seus funcionários. O setor de recursos humanos, para poder alimentar a base de dados de pagamento, obterá um nível diferente de acesso e sua interação com o sistema será feita a partir de menus próprios para a administração de pessoal. Os menus apresentados após a seleção de uma das opções (funcionário, gerente ou setor de recursos humanos) serão, portanto, diferentes.

1.6.2.. Para que servem os controles de funções de aplicativos?

No que diz respeito às funções internas dos aplicativos, os respectivos proprietários deverão definir quem poderá acessá-las e como, através de autorização para uso de funções específicas ou restrição de acesso a funções de acordo com o usuário (menus de acesso predefinidos), horário ou tipo de recursos (impressoras, fitas backup).

1.6.3. Como proteger arquivos?

A maioria dos sistemas operacionais possui mecanismos de controle de acesso que definem as permissões e os privilégios de acesso para cada recurso ou arquivo no sistema. Quando um usuário

tenta acessar um recurso, o sistema operacional verifica se as definições de acesso desse usuário e do recurso desejado conferem. O usuário só conseguirá o acesso se essa verificação for positiva.

Para garantir a segurança lógica, pode-se especificar dois tipos de controle, sob óticas diferentes :

- O que um sujeito pode fazer; ou
- O que pode ser feito com um objeto.

1.6.4. O que são direitos e permissões de acesso?

Definir direitos de acesso individualmente para cada sujeito e objeto pode ser uma maneira um tanto trabalhosa quando estiverem envolvidas grandes quantidades de sujeitos e objetos. A forma mais comum de definição de direitos de acesso, nesse caso, é a matriz de controle de acesso. Nessa matriz pode-se fazer duas análises : uma em relação aos sujeitos; outra, em relação aos objetos.

Na primeira abordagem, cada sujeito recebe uma permissão (ou capacidade) que define todos os seus direitos de acesso. As permissões de acesso são, então, atributos, associados a um sujeito ou objeto, que definem o que ele pode ou não fazer com outros objetos. Essa abordagem, no entanto, é pouco utilizada, já que, na prática, com grandes quantidades de sujeitos e objetos, a visualização exata de quem tem acesso a um determinado objeto não é tão clara, comprometendo, assim, a gerência de controle de acesso.

Na segunda abordagem, os direitos de acesso são armazenados com o próprio objeto formando a chamada lista de controle de acesso (ACL - *Access Control List*).

1.6.5. O que são listas de controle de acesso?

Enquanto a permissão de acesso define o que um objeto pode ou não fazer com outros, a lista de controle de acesso define o que os outros objetos ou sujeitos podem fazer com o objeto a ela associado. As listas de controle de acesso nada mais são do que bases de dados, associadas a um objeto, que descrevem os relacionamentos entre aquele objeto e outros, constituindo-se em um mecanismo de garantia de confidencialidade e integridade de dados.

A definição das listas de controle de acesso deve ser sempre feita pelos proprietários dos recursos, os quais determinam o tipo de proteção adequada a cada recurso e quem efetivamente terá acesso a eles.

A gerência das listas de controle de acesso, na prática, também é complicada. Para reduzir os problemas de gerenciamento dessas listas e o espaço de memória ou disco por elas ocupado, costuma-se agrupar os sujeitos com características semelhantes ou direitos de acesso iguais. Dessa forma, os direitos de acesso são associados a grupos, e não a sujeitos individualizados. Vale ressaltar que um sujeito pode pertencer a um ou mais grupos, de acordo com o objeto a ser acessado.

1.7 Como monitorar o acesso aos recursos informacionais?

O monitoramento dos sistemas de informação é feito, normalmente, através de registros de log, trilhas de auditoria ou outros mecanismos capazes de detectar invasões. Esse monitoramento é essencial à equipe de segurança de informações, já que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários.

Na ocorrência de uma invasão, falha do sistema ou atividade não autorizada, é imprescindível reunir evidências suficientes para que possam ser tomadas medidas corretivas necessárias ao restabelecimento do sistema às suas condições normais, assim como medidas administrativas e/ou judiciais para investigar e punir os invasores.

A forma mais simples de monitoramento é a coleta de informações, sobre determinados eventos, em arquivos históricos, mais conhecidos como logs. Com essas informações, a equipe de segurança é capaz de registrar eventos e detectar tentativas de acesso e atividades não autorizadas após sua ocorrência.

1.7.1. O que são logs?

Os logs são registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim.

Os logs são utilizados como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou

de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando. Com os dados dos logs, pode-se identificar e corrigir falhas da estratégia de segurança. Por conterem informações essenciais para a detecção de acesso não autorizado, os arquivos de log devem ser protegidos contra alteração ou destruição por usuários ou invasores que queiram encobrir suas atividades.

1.7.2. O que deve ser registrado em logs?

Devido à grande quantidade de dados armazenada em logs, deve-se levar em consideração que seu uso pode degradar o desempenho dos sistemas. Sendo assim, é aconselhável balancear a necessidade de registro de atividades críticas e os custos, em termos de desempenho global dos sistemas. Normalmente, os registros de log incluem:

- identificação dos usuários;
- datas e horários de entrada (logon) e saída do sistema (logoff);
- identificação da estação de trabalho e, quando possível, sua localização;
- registros das tentativas de acesso (aceitas e rejeitadas) ao sistema;
- registros das tentativas de acesso (aceitas e rejeitadas) a outros recursos e dados.

Ao definir o que será registrado, é preciso considerar que quantidades enormes de registros podem ser inviáveis de serem monitoradas. Nada adianta ter um log se ele não é periodicamente revisado. Para auxiliar a gerência de segurança na árdua tarefa de análise de logs, podem ser previamente definidas trilhas de auditoria mais simples e utilizados softwares especializados disponíveis no mercado, específicos para cada sistema operacional.

1.8. Outros controles de acesso lógico

Outro recurso de proteção bastante utilizado em alguns sistemas é o time-out automático, isto é, a sessão é desativada após um determinado tempo sem qualquer atividade no terminal ou computador. Para restaurá-la, o usuário é obrigado a fornecer novamente seu ID e senha. Em alguns sistemas operacionais, o próprio usuário, após sua habilitação no processo de logon, pode ativar e desativar essa função de time-out. Nesse sentido, os usuários devem ser orientados a:

- encerrar as sessões ativas, a menos que elas possam ser protegidas por mecanismo de bloqueio (por exemplo, proteção de tela com senha);
- no caso de terminal conectado a computador de grande porte, efetuar a desconexão quando a sessão for finalizada (não apenas desligar o terminal, mas utilizar o procedimento para desconexão).

Como controle de acesso lógico, a gerência de segurança pode ainda limitar o horário de uso dos recursos computacionais de acordo com a real necessidade de acesso aos sistemas.

Pode-se, por exemplo, desabilitar o uso dos recursos nos fins de semana ou à noite.

É usual também limitar a quantidade de sessões concorrentes, impedindo que o usuário consiga entrar no sistema ou na rede a partir de mais de um terminal ou computador simultaneamente. Isso reduz os riscos de acesso ao sistema por invasores, pois se o usuário autorizado já estiver conectado, o invasor não poderá entrar no sistema. Da mesma forma, se o invasor estiver logado, o usuário autorizado, ao tentar se conectar, identificará que sua conta já está sendo usada e poderá notificar o fato à gerência de segurança.

1.9. Onde as regras de controle de acesso são definidas?

As regras de controle e direitos de acesso para cada usuário ou grupo devem estar claramente definidas no documento da política de controle de acesso da instituição, o qual deverá ser fornecido aos usuários e provedores de serviço para que tomem conhecimento dos requisitos de segurança estabelecidos pela gerência.

1.9.1. O que considerar na elaboração da política de controle de acesso?

A política de controle de acesso deve levar em conta:

- os requisitos de segurança de aplicações específicas do negócio da instituição;
- a identificação de toda informação referente às aplicações de negócio;

- as políticas para autorização e distribuição de informação (por exemplo, a necessidade de conhecer os princípios e níveis de segurança, bem como a classificação da informação);

- a compatibilidade entre o controle de acesso e as políticas de classificação da informação dos diferentes sistemas e redes;

- a legislação vigente e qualquer obrigação contratual considerando a proteção do acesso a dados ou serviços;

- o perfil de acesso padrão para categorias de usuários comuns;

- o gerenciamento dos direitos de acesso em todos os tipos de conexões disponíveis em um ambiente distribuído conectado em rede.

1.9.2. Que cuidados devem ser tomados na definição das regras de controle de acesso?

Ao especificar as regras de controle de acesso, devem ser considerados os seguintes aspectos:

- diferenciar regras que sempre devem ser cumpridas das regras opcionais ou condicionais;

- estabelecer regras baseadas na premissa “Tudo deve ser proibido a menos que expressamente permitido” ao invés da regra “Tudo é permitido a menos que expressamente proibido”;

- diferenciar as permissões de usuários que são atribuídas automaticamente por um sistema de in-

formação daquelas atribuídas por um administrador;

- priorizar regras que necessitam da aprovação de um administrador antes da liberação daquelas que não necessitam de tal aprovação.

1.9.3. Que tipo de regras de controle de acesso devem ser formalizadas na política?

O acesso aos sistemas de informação deve ser controlado através de um processo formal, o qual deverá abordar, entre outros, os seguintes tópicos:

- utilização de um identificador de usuário (ID) único, de forma que cada usuário possa ser identificado e responsabilizado por suas ações;

- verificação se o usuário obteve autorização do proprietário do sistema de informação ou serviço para sua utilização;

- verificação se o nível de acesso concedido ao usuário está adequado aos propósitos do negócio e consistente com a política de segurança da organização;

- fornecimento, aos usuários, de documento escrito com seus direitos de acesso. Os usuários deverão assinar esse documento, indicando que entenderam as condições de seus direitos de acesso;

- manutenção de um registro formal de todas as pessoas cadastradas para usar cada sistema de informações;

- remoção imediata dos direitos de acesso de usuários que mudarem de função ou saírem da organização;

- verificação periódica da lista de usuários, com intuito de remover usuários inexistentes e IDs em duplicidade;

- inclusão de cláusulas nos contratos de funcionários e prestadores de serviço, que especifiquem as sanções a que estarão sujeitos em caso de tentativa de acesso não autorizado.

1.10. Quem é o responsável pelos controles de acesso lógico?

A responsabilidade sobre os controles de acesso lógico pode ser tanto do gerente do ambiente operacional como dos proprietários (ou gerentes) de aplicativos. O gerente do ambiente operacional deve controlar o acesso à rede, ao sistema operacional e seus recursos e, ainda, aos aplicativos e arquivos de dados. É responsável, assim, por proteger os recursos do sistema contra invasores ou funcionários não autorizados.

Enquanto isso, os proprietários dos aplicativos são responsáveis por seu controle de acesso, identificando quem pode acessar cada um dos sistemas e que tipo de operações pode executar. Por conhecerem bem o sistema aplicativo sob sua responsabilidade, os proprietários são as pessoas mais indicadas para definir privilégios de acesso de acordo com as reais necessidades dos usuários.

Dessa forma, as responsabilidades sobre segurança de acesso são segregadas entre o gerente do ambiente operacional de informática e os gerentes de aplicativos.

1.1.1. Em que os usuários podem ajudar na implantação dos controles de acesso lógico?

A cooperação dos usuários autorizados é essencial para a eficácia da segurança. Os usuários devem estar cientes de suas responsabilidades para a manutenção efetiva dos controles de acesso, considerando, particularmente, o uso de senhas e a segurança dos equipamentos de informática que costumam utilizar.

1.1.2. Referências bibliográficas

1. ABNT. *NBR ISO/IEC 17799 - Tecnologia da informação: código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2001.
2. DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000. 218p.

2. Política de Segurança de Informações

Neste Capítulo serão apresentados conceitos relativos à política de segurança de informações, bem como questões que demonstram a importância de sua elaboração, implementação e divulgação.

2.1. O que visa a segurança de informações?

A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas com os controles de acesso abordados no Capítulo 1.

2.1.1. O que é integridade de informações?

Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos

pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

2.1.2. O que é confidencialidade de informações?

Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

2.1.3. O que é autenticidade de informações?

Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

2.1.4. O que é disponibilidade de informações?

Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem de direito.

2.2. Por que é importante zelar pela segurança de informações?

Porque a informação é um ativo muito importante para qualquer organização, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da organização perante terceiros, como também o andamento dos próprios processos organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações.

2.3. O que é política de segurança de informações - PSI?

Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos.

As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações.

2.4. Quem são os responsáveis por elaborar a PSI?

É recomendável que na estrutura da organização exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança.

Vale salientar, entretanto, que pessoas de áreas críticas da organização devem participar do processo de elaboração da PSI, como a alta administração e os diversos gerentes e proprietários dos sistemas informatizados. Além disso, é recomendável que a PSI seja aprovada pelo mais alto dirigente da organização.

2.5. Que assuntos devem ser abordados na PSI?

A política de segurança de informações deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e recursos computacionais. Ela não deve ficar restrita à área de informática. Ao contrário, ela deve estar integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da organização concernentes à segurança em geral.

O conteúdo da PSI varia, de organização para organização, em função de seu estágio de maturidade, grau de informatização, área de atuação, cultura organizacional, necessidades requeridas, requisitos de segurança, entre outros aspectos. No entanto, é comum a presença de alguns tópicos na PSI, tais como:

- definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- objetivos de segurança da organização;
- definição de responsabilidades gerais na gestão de segurança de informações;
- orientações sobre análise e gestão de riscos;
- princípios de conformidade dos sistemas computacionais com a PSI;
- padrões mínimos de qualidade que esses sistemas devem possuir;
- políticas de controle de acesso a recursos e sistemas computacionais;
- classificação das informações (de uso irrestrito, interno, confidencial e secretas);
- procedimentos de prevenção e detecção de vírus;

- princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);

- princípios de supervisão constante das tentativas de violação da segurança de informações;

- consequências de violações de normas estabelecidas na política de segurança;

- princípios de gestão da continuidade do negócio;

- plano de treinamento em segurança de informações.

2.6. Qual o nível de profundidade que os assuntos abordados na PSI devem ter?

A política de segurança de informações deve conter princípios, diretrizes e regras genéricos e amplos, para aplicação em toda a organização. Além disso, ela deve ser clara o suficiente para ser bem compreendida pelo leitor em foco, aplicável e de fácil aceitação. A complexidade e extensão exageradas da PSI pode levar ao fracasso de sua implementação.

Cabe destacar que a PSI pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares.

Ademais, quando a organização achar conveniente e necessário que sua PSI seja mais abrangente e detalhada, sugere-se a criação de outros documentos que especifiquem práticas e procedimentos e que descrevam com mais detalhes as regras de uso da tecnologia da informação. Esses documentos costumam dispor sobre regras mais específicas, que detalham as responsabilidades dos usuários, gerentes e auditores e, normalmente, são atualizados com maior frequência. A PSI é o primeiro de muitos documentos com informações cada vez mais detalhadas sobre procedimentos, práticas e padrões a serem aplicados em determinadas circunstâncias, sistemas ou recursos.

2.7. Como se dá o processo de implantação da PSI?

O processo de implantação da política de segurança de informações deve ser formal. No decorrer desse processo, a PSI deve permanecer passível a ajustes para melhor adaptar-se às reais necessidades. O tempo desde o início até a completa implantação tende a ser longo. Em resumo, as principais etapas que conduzem à implantação bem sucedida da PSI são: elaboração, aprovação, implementação, divulgação e manutenção. Muita atenção deve ser dada às duas últimas etapas, haja vista ser comum sua não observância. Normalmente, após a consecução das três primeiras etapas, as gerências de segurança acreditam terem cumprido o dever e esquecem da importância da divulgação e atualização da PSI.

De forma mais detalhada, pode-se citar como as principais fases que compõem o processo de implantação da PSI:

- identificação dos recursos críticos;
- classificação das informações;
- definição, em linhas gerais, dos objetivos de segurança a serem atingidos;
- análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos);
- elaboração de proposta de política;
- discussões abertas com os envolvidos;
- apresentação de documento formal à gerência superior;
- aprovação;
- publicação;
- divulgação;
- treinamento;
- implementação;
- avaliação e identificação das mudanças necessárias;
- revisão.

2.8. Qual o papel da alta administração na elaboração e implantação da PSI?

O sucesso da PSI está diretamente relacionado com o envolvimento e a atuação da alta administração. Quanto maior for o comprometimento da gerência superior com os processos de elaboração e implantação da PSI, maior a probabilidade de ela ser efetiva e eficaz. Esse comprometimento deve ser expresso formalmente, por escrito.

2.9. A quem deve ser divulgada a PSI?

A divulgação ampla a todos os usuários internos e externos à organização é um passo indispensável para que o processo de implantação da PSI tenha sucesso. A PSI deve ser de conhecimento de todos que interagem com a organização e que, direta ou indiretamente, serão afetados por ela. É necessário que fique bastante claro, para todos, as conseqüências advindas do uso inadequado dos sistemas computacionais e de informações, as medidas preventivas e corretivas que estão a seu cargo para o bom, regular e efetivo controle dos ativos computacionais. A PSI fornece orientação básica aos agentes envolvidos de como agir corretamente para atender às regras nela estabelecidas. É importante, ainda, que a PSI esteja permanentemente acessível a todos.

2.10. O que fazer quando a PSI for violada?

A própria Política de Segurança de Informações deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com sua severidade, amplitude e tipo de infrator que a perpetra. A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial.

A Lei n.º 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro, já prevê penas para os casos de violação de integridade e quebra de sigilo de sistemas informatizados ou banco de dados da Administração Pública. O novo art. 313-A trata da inserção de dados falsos em sistemas de informação, enquanto o art. 313-B discorre sobre a modificação ou alteração não autorizada desses mesmos sistemas. O § 1º do art. 153 do Código Penal foi alterado e, atualmente, define penas quando da divulgação de informações sigilosas ou reservadas, contidas ou não nos bancos de dados da Administração Pública. O fornecimento ou empréstimo de senha que possibilite o acesso de pessoas não autorizadas a sistemas de informações é tratado no inciso I do § 1º do art. 325 do Código Penal.

Neste tópico, fica ainda mais evidente a importância da conscientização dos funcionários quanto à PSI. Uma vez que a Política seja de conhecimento de todos da organização, não será admissível que as pessoas aleguem ignorância quanto às regras nela estabelecidas a fim de livrar-se da culpa sobre violações cometidas.

Quando detectada uma violação, é preciso averiguar suas causas, conseqüências e circunstâncias em que ocorreu. Pode ter sido derivada de um simples acidente, erro ou mesmo desconhecimento da PSI, como também de negligência, ação deliberada e fraudulenta. Essa averiguação possibilita que vulnerabilidades até então desconhecidas pelo pessoal da gerência de segurança passem a ser consideradas, exigindo, se for o caso, alterações na PSI.

2.11. Uma vez definida, a PSI pode ser alterada?

A PSI não só pode ser alterada, como deve passar por processo de revisão definido e periódico que garanta sua reavaliação a qualquer mudança que venha afetar a análise de risco original, tais como: incidente de segurança significativo, novas vulnerabilidades, mudanças organizacionais ou na infra-estrutura tecnológica. Além disso, deve haver análise periódica da efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados. É desejável, também, que sejam avaliados o custo e o impacto dos controles na eficiência do negócio, a fim de que esta não seja comprometida pelo excesso ou escassez de controles.

É importante frisar, ainda, que a PSI deve ter um gestor responsável por sua manutenção e análise crítica.

2.12. Existem normas sobre PSI para a Administração Pública Federal?

O Decreto n.º 3.505, de 13.06.2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Em linhas gerais, os objetivos traçados nessa PSI dizem respeito à necessidade de capacitação e conscientização das pessoas lotadas nos órgãos e entidades da Administração Pública Federal quanto aos aspectos de segurança da informação; e necessidade de elaboração e edição de instrumentos jurídicos, normativos e organizacionais que promo-

vam a efetiva implementação da segurança da informação. Com relação às matérias que esses instrumentos devem versar, o Decreto menciona:

- padrões relacionados ao emprego dos produtos que incorporam recursos criptográficos;
- normas gerais para uso e comercialização dos recursos criptográficos;
- normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados;
- normas relacionadas à emissão de certificados de conformidade;
- normas relativas à implementação dos sistemas de segurança da informação, com intuito de garantir a sua interoperabilidade, obtenção dos níveis de segurança desejados e permanente disponibilização dos dados de interesse para a defesa nacional;

Além disso, o Decreto prevê a concepção, especificação e implementação da infra-estrutura de chaves públicas - ICP a ser utilizada pelos órgãos e entidades da Administração Pública Federal. Em 28 de junho de 2001, foi editada a Medida Provisória n.º 2.200, que institui a Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Os principais objetivos do ICP Brasil são: assegurar a confidencialidade, a autenticidade e a integridade das mensagens e documentos eletrônicos, e evitar que deixem de ser honrados compromissos assumidos mediante sua utilização. Pretende-se difundir um rigoroso sistema de informática que armazene e identifique os dados transmitidos eletronicamente, as chamadas assinaturas digitais, compostas por chave pública e chave privada. Além disso, foi editado, em 31 de outubro de 2001, o Decreto n.º 3.996, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

2.13. Referências bibliográficas

1. ABNT. *NBR ISO/IEC 17799 - Tecnologia da informação: código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2001.
2. DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000. 218p.
3. BRASIL. Decreto n.º 3.505, de 13 de junho de 2000. [Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal].
4. _____. Decreto n.º 3.996, de 31 de outubro de 2001. [Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal].
5. _____. Lei n.º 9.983, de 14 de julho de 2000. [Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências].
6. _____. Medida Provisória n.º 2.200-2, de 24 de agosto de 2001. [Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências].

3. Plano de Contingências

Neste Capítulo será apresentada a importância de definição de estratégias que permitam que uma instituição retorne à sua normalidade, em caso de acontecimento de situações inesperadas.

3.1. O que é Plano de Contingências?

Plano de Contingências consiste num conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços. Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade. O Plano de Contingências é um conjunto de medidas que combinam ações preventivas e de recuperação.

Obviamente, os tipos de riscos a que estão sujeitas as organizações variam no tempo e no espaço. Porém, pode-se citar como exemplos de riscos mais

comuns a ocorrência de desastres naturais (enchentes, terremotos, furacões), incêndios, desabamentos, falhas de equipamentos, acidentes, greves, terrorismo, sabotagem, ações intencionais.

O Plano de Contingências pode ser desenvolvido por organizações que contenham ou não sistemas computadorizados. Porém, para efeito desta cartilha, o Plano se aplica às organizações que, em menor ou maior grau, dependem da tecnologia da informação, pois faz-se referência aos riscos a que essa área está sujeita, bem como aos aspectos relevantes para superar problemas decorrentes.

3.2. Qual é a importância do Plano de Contingências?

Atualmente, é inquestionável a dependência das organizações aos computadores, sejam eles de pequeno, médio ou grande porte. Essa característica quase generalizada, por si só, já é capaz de explicar a importância do Plano de Contingências, pois se para fins de manutenção de seus serviços, as organizações dependem de computadores e de infor-

mações armazenadas em meio eletrônico, o que fazer na ocorrência de situações inesperadas que comprometam o processamento ou disponibilidade desses computadores ou informações? Ao contrário do que ocorria antigamente, os funcionários não mais detêm o conhecimento integral, assim como a habilidade para consecução dos processos organizacionais, pois eles são, muitas vezes, executados de forma transparente. Além disso, as informações não mais se restringem ao papel, ao contrário, elas estão estrategicamente organizadas em arquivos magnéticos.

Por conseguinte, pode-se considerar o Plano de Contingências quesito essencial para as organizações preocupadas com a segurança de suas informações.

3.3. Qual é o objetivo do Plano de Contingências?

O objetivo do Plano de Contingências é manter a integridade e a disponibilidade dos dados da organização, bem como a disponibilidade dos seus serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento dos negócios. Possui como objetivo, ainda, garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos. É normal que, em determinadas situações de anormalidade, o Plano preveja a possibilidade de fornecimento de serviços temporários ou com restrições, que, pelo menos, supram as necessidades imediatas e mais críticas.

Cabe destacar que o Plano é um entre vários requisitos de segurança necessários para que os aspectos de integridade e disponibilidade sejam preservados durante todo o tempo.

3.4. Como iniciar a elaboração do Plano de Contingências?

Antes da elaboração do Plano de Contingências propriamente dito, é importante analisar alguns aspectos:

- riscos a que está exposta a organização, probabilidade de ocorrência e os impactos decorrentes (tanto aqueles relativos à escala do dano como ao tempo de recuperação);
- conseqüências que poderão advir da interrupção de cada sistema computacional;
- identificação e priorização de recursos, sistemas, processos críticos;
- tempo limite para recuperação dos recursos, sistemas, processos;
- alternativas para recuperação dos recursos, sistemas, processos, mensurando os custos e benefícios de cada alternativa.

3.5. Que assuntos devem ser abordados no Plano de Contingências?

De maneira geral, o Plano de Contingências contém informações sobre:

- condições e procedimentos para ativação do Plano (como se avaliar a situação provocada por um incidente);
- procedimentos a serem seguidos imediatamente após a ocorrência de um desastre (como, por exemplo, contato eficaz com as autoridades públicas apropriadas: polícia, bombeiro, governo local);
- a instalação reserva, com especificação dos bens de informática nela disponíveis, como hardware, software e equipamentos de telecomunicações;
- a escala de prioridade dos aplicativos, de acordo com seu grau de interferência nos resultados operacionais e financeiros da organização. Quanto mais o aplicativo influenciar na capacidade de funcionamento da organização, na sua situação econômica e na sua imagem, mais crítico ele será;
- arquivos, programas, procedimentos necessários para que os aplicativos críticos entrem em operação no menor tempo possível, mesmo que parcialmente;
- sistema operacional, utilitários e recursos de telecomunicações necessários para assegurar o processamento dos aplicativos críticos, em grau pré-estabelecido;
- documentação dos aplicativos críticos, sistema operacional e utilitários, bem como suprimentos de informática, ambos disponíveis na instalação reserva e capazes de garantir a boa execução dos processos definidos;
- dependência de recursos e serviços externos ao negócio;
- procedimentos necessários para restaurar os serviços computacionais na instalação reserva;
- pessoas responsáveis por executar e comandar cada uma das atividades previstas no Plano (é interessante definir suplentes, quando se julgar necessário);
- referências para contato dos responsáveis, sejam eles funcionários ou terceiros;
- organizações responsáveis por oferecer serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração;
- contratos e acordos que façam parte do plano para recuperação dos serviços, como aqueles efetuados com outros centros de processamento de dados.

3.6. Qual o papel da alta gerência na elaboração do Plano de Contingências?

É imprescindível o comprometimento da alta administração com o Plano de Contingências. Na verdade, este Plano é de responsabilidade direta da alta gerência, é um problema corporativo, pois trata-se de estabelecimento de procedimentos que garantirão a sobrevivência da organização como um todo e não apenas da área de informática. Ainda, muitas das definições a serem especificadas são definições relativas ao negócio da organização e não à tecnologia da informação.

A alta gerência deve designar uma equipe de segurança específica para elaboração, implementação, divulgação, treinamento, testes, manutenção e coordenação do Plano de Contingências. Este deve possuir, ainda, um responsável específico que esteja a frente das demandas, negociações e tudo mais que se fizer necessário.

Provavelmente, a alta gerência será demandada a firmar acordos de cooperação com outras organizações, assinar contratos orientados para a recuperação dos serviços, entre outros atos.

Há que ser considerada, ainda, a questão dos custos. Faz parte das decisões da alta gerência o orçamento a ser disponibilizado para garantir a exequibilidade do Plano de Contingências, ou seja, para possibilitar, além da sua implementação, sua manutenção, treinamento e testes.

Diante dos fatos anteriormente abordados, fica evidente a necessidade precípua de envolvimento da alta gerência com todo processo que garantirá o sucesso de implantação do Plano de Contingências.

3.7. Como garantir que o Plano funcionará como esperado?

É possível citar três formas de garantir a eficácia do Plano de Contingências: treinamento e conscientização das pessoas envolvidas; testes periódicos do Plano, integrais e parciais; processo de manutenção contínua.

3.7.1. Como deve ser realizado o treinamento e a conscientização das pessoas?

É essencial o desenvolvimento de atividades educativas e de conscientização que visem ao perfeito entendimento do processo de continuidade de serviços e que garantam, por conseguinte, a efetividade do Plano de Contingências.

Cada funcionário envolvido com o processo de continuidade de serviços, especialmente aqueles componentes de equipes com responsabilidades específicas em caso de contingências, deve ter em mente as atividades que deve desempenhar em situações emergenciais. O treinamento deve ser teórico e prático, inclusive com simulações. Além do treinamento, a conscientização pode ser feita de outras formas, como distribuição de folhetos e promoção de palestras informativas e educativas sobre possíveis acidentes e respectivos planos de recuperação.

Por fim, vale salientar que um programa de educação continuada que faça com que as pessoas envolvidas sintam-se como participantes ativos do programa de segurança é a melhor maneira de alcançar o sucesso esperado.

3.7.2. Por que o Plano de Contingências deve ser testado?

Os planos de continuidade do negócio podem apresentar falhas quando testados, geralmente devido a pressupostos incorretos, omissões ou mudanças de equipamentos, de pessoal, de prioridades. Por isto eles devem ser testados regularmente, de forma a garantir sua permanente atualização e efetividade. Tais testes também devem assegurar que todos os envolvidos na recuperação e os alocados em outras funções críticas possuam conhecimento do Plano.

Deve existir uma programação que especifique quando e como o Plano de Contingências deverá ser testado. Ele pode ser testado na sua totalidade, caracterizando uma situação bem próxima da realidade; pode ser testado parcialmente, quando restringem-se os testes a apenas um conjunto de procedimentos, atividades ou aplicativos componentes do Plano; ou, ainda, pode ser testado por meio de simulações, quando ocorre representações de situação emergencial. A partir da avaliação dos resultados dos testes, é possível reavaliar o Plano, alterá-lo e adequá-lo, se for o caso.

3.7.3. Que fatos podem provocar a necessidade de atualização do Plano de Contingências?

Mudanças que tenham ocorrido e que não estejam contempladas no Plano de Contingências devem gerar atualizações. Quando novos requisitos forem identificados, os procedimentos de emergência relacionados devem ser ajustados de forma apropriada. Diversas situações podem demandar atualizações no Plano, tais como as mudanças:

- no parque ou ambiente computacional (ex: aquisição de novo equipamento, atualização de sistemas operacionais, migração de sistemas de grande porte para ambiente cliente-servidor);
- administrativas, de pessoas envolvidas e responsabilidades;
- de endereços ou números telefônicos;

- de estratégia de negócio;
- na localização e instalações;
- na legislação;
- em prestadores de serviço, fornecedores e clientes-chave;
- de processos (inclusões e exclusões);
- no risco (operacional e financeiro).

Como demonstrado, as atualizações regulares do Plano de Contingências são de importância fundamental para alcançar a sua efetividade. Deve existir uma programação que especifique a forma de se proceder à manutenção do Plano. Procedimentos com essa finalidade podem ser incluídos no processo de gerência de mudanças a fim de que as questões relativas à continuidade de negócios sejam devidamente tratadas. O controle formal de mudanças permite assegurar que o processo de atualização esteja distribuído e garantido por revisões periódicas do Plano como um todo. A responsabilidade pelas revisões e atualizações de cada parte do Plano deve ser definida e estabelecida.

3.8. Referências bibliográficas

1. ABNT. *NBR ISO/IEC 17799 - Tecnologia da informação: código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2001.
2. DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000. 218p.

Cláudia Augusto Dias

Mestre em Ciência da Informação, graduada em Engenharia Elétrica (Universidade de Brasília). Trabalha como Analista de Controle Externo no Tribunal de Contas da União, no Projeto Portal TCU.

Roberta Ribeiro de Queiroz Martins

Graduada em Ciência da Computação pela Universidade Católica de Pernambuco. Atua há cinco anos em Auditoria da Tecnologia da Informação no TCU, sendo, atualmente, integrante de Diretoria específica nessa área.

4. Anexos

Presidência da República
Subchefia para Assuntos Jurídicos

DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000.

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e tendo em vista o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 2.910, de 29 de dezembro de 1998,

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:

I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;

V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e

VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I - Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Art. 3º São objetivos da Política da Informação:

I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

V - promover as ações necessárias à implementação e manutenção da segurança da informação;

VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

Art. 4º Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6º, adotar as seguintes diretrizes:

I - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;

II - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;

III - propor regulamentação sobre matérias afetas à segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

IV - estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;

V - acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;

VI - orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;

VII - realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;

VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;

IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;

X - estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;

XI - estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;

XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;

XIII - estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; e

XIV - conceber, especificar e coordenar a implementação da infra-estrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal.

Art. 5º À Agência Brasileira de Inteligência - ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC, competirá:

I - apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação; e

II - integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Art. 6º Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto.

Art. 7º O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados:

I - Ministério da Justiça;

II - Ministério da Defesa;

III - Ministério das Relações Exteriores;

IV - Ministério da Fazenda;

V - Ministério da Previdência e Assistência Social;

VI - Ministério da Saúde;

VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VIII - Ministério do Planejamento, Orçamento e Gestão;

IX - Ministério das Comunicações;

X - Ministério da Ciência e Tecnologia;

XI - Casa Civil da Presidência da República; e

XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará.

§ 1º Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados.

§ 2º Os membros do Comitê Gestor não poderão participar de processos similares de iniciativa do setor privado, exceto nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República.

§ 3º A participação no Comitê não enseja remuneração de qualquer espécie, sendo considerada serviço público relevante.

§ 4º A organização e o funcionamento do Comitê serão dispostos em regimento interno por ele aprovado.

§ 5º Caso necessário, o Comitê Gestor poderá propor a alteração de sua composição.

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Brasília, 13 de junho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO

José Gregori

Geraldo Magela da Cruz Quintão

Luiz Felipe Lampreia

Pedro Malan

Waldeck Ornélas

José Serra

Alcides Lopes Tápias

Martus Tavares

Pimenta da Veiga

Ronaldo Mota Sardenberg

Pedro Parente

Alberto Mendes Cardoso

Publicado no D.O. de 14.6.2000

**Presidência da República
Subchefia para Assuntos Jurídicos**

LEI Nº 9.983, DE 14 DE JULHO DE 2000.

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º São acrescidos à Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, os seguintes dispositivos:

“Apropriação indébita previdenciária” (AC)*

“Art. 168-A. Deixar de repassar à previdência social as contribuições recolhidas dos contribuintes, no prazo e forma legal ou convencional:” (AC)

“Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.” (AC)

“§ 1º Nas mesmas penas incorre quem deixar de:” (AC)

“I – recolher, no prazo legal, contribuição ou outra importância destinada à previdência social que tenha sido descontada de pagamento efetuado a segurados, a terceiros ou arrecadada do público;” (AC)

“II – recolher contribuições devidas à previdência social que tenham integrado despesas contábeis ou custos relativos à venda de produtos ou à prestação de serviços;” (AC)

“III - pagar benefício devido a segurado, quando as respectivas cotas ou valores já tiverem sido reembolsados à empresa pela previdência social.” (AC)

“§ 2º É extinta a punibilidade se o agente, espontaneamente, declara, confessa e efetua o pagamento das contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal.” (AC)

“§ 3º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:” (AC)

“I – tenha promovido, após o início da ação fiscal e antes de oferecida a denúncia, o pagamento da contribuição social previdenciária, inclusive acessórios; ou” (AC)

“II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais.” (AC)

“Inserção de dados falsos em sistema de informações” (AC)

“Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:” (AC)

“Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.” (AC)

“Modificação ou alteração não autorizada

de sistema de informações” (AC)

“Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:” (AC)

“Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.” (AC)

“Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.” (AC)

“Sonegação de contribuição previdenciária” (AC)

“Art. 337-A. Suprimir ou reduzir contribuição social previdenciária e qualquer acessório, mediante as seguintes condutas:” (AC)

“I – omitir de folha de pagamento da empresa ou de documento de informações previsto pela legislação previdenciária segurados empregado, empresário, trabalhador avulso ou trabalhador autônomo ou a este equiparado que lhe prestem serviços;” (AC)

“II – deixar de lançar mensalmente nos títulos próprios da contabilidade da empresa as quantias descontadas dos segurados ou as devidas pelo empregador ou pelo tomador de serviços;” (AC)

“III – omitir, total ou parcialmente, receitas ou lucros auferidos, remunerações pagas ou creditadas e demais fatos geradores de contribuições sociais previdenciárias.” (AC)

“Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.” (AC)

“§ 1º É extinta a punibilidade se o agente, espontaneamente, declara e confessa as contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal.” (AC)

“§ 2º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:” (AC)

“I – (VETADO)”

“II – o valor das contribuições devidas, inclusive acessórias, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais.” (AC)

“§ 3º Se o empregador não é pessoa jurídica e sua folha de pagamento mensal não ultrapassa R\$ 1.510,00 (um mil, quinhentos e dez reais), o juiz poderá reduzir a pena de um terço até a metade ou aplicar apenas a de multa.” (AC)

“§ 4º O valor a que se refere o parágrafo anterior será reajustado nas mesmas datas e nos mesmos índices do reajuste dos benefícios da previdência social.” (AC)

Art. 2º Os arts. 153, 296, 297, 325 e 327 do Decreto-Lei nº 2.848, de 1940, passam a vigorar com as seguintes alterações:

“Art. 153.”

“§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.” (AC)

“Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.” (AC)

“§ 1º (parágrafo único original).....”

“§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.” (AC)

“Art. 296.”

“§ 1º

.....”

“III – quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública.” (AC)

“.....”

“Art. 297.

.....”

“§ 3º Nas mesmas penas incorre quem insere ou faz inserir:” (AC)

“I – na folha de pagamento ou em documento de informações que seja destinado a fazer prova perante a previdência social, pessoa que não possua a qualidade de segurado obrigatório;” (AC)

“II – na Carteira de Trabalho e Previdência Social do empregado ou em documento que deva produzir efeito perante a previdência social, declaração falsa ou diversa da que deveria ter sido escrita;” (AC)

“III – em documento contábil ou em qualquer outro documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado.” (AC)

“§ 4º Nas mesmas penas incorre quem omite, nos documentos mencionados no § 3º, nome do segurado e seus dados pessoais, a remuneração, a vigência do contrato de trabalho ou de prestação de serviços.” (AC)

“Art. 325.”

“§ 1º Nas mesmas penas deste artigo incorre quem:” (AC)

“I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer

outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;” (AC)

“II – se utiliza, indevidamente, do acesso restrito.” (AC)

“§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:” (AC)

“Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.” (AC)

“Art. 327.”

“§ 1º Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.” (NR)

“.....”

Art. 3º O art. 95 da Lei nº 8.212, de 24 de julho de 1991, passa a vigorar com a seguinte redação:

“Art. 95. *Caput.* Revogado.”

“a) revogada;”

“b) revogada;”

“c) revogada;”

“d) revogada;”

“e) revogada;”

“f) revogada;”

“g) revogada;”

“h) revogada;”

“i) revogada;”

“j) revogada.”

“§ 1º Revogado.”

“§ 2º”

“a)”

“b)”

“c)”

“d)”

“e)”

“f)”

“§ 3º Revogado.”

“§ 4º Revogado.”

“§ 5º Revogado.”

Art. 4º Esta Lei entra em vigor noventa dias após a data de sua publicação.

Brasília, 14 de julho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO

José Gregori

Waldeck Ornelas

Publicado no D.O. de 17.7.2000

Presidência da República
Subchefia para Assuntos Jurídicos

DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000.

Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov será instituída nos termos deste Decreto.

Art. 2º A tecnologia da ICP-Gov deverá utilizar criptografia assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade.

§ 1º A criptografia utilizará duas chaves matematicamente relacionadas, onde uma delas é pública e, a outra, privada, para criação de assinatura digital, com a qual será possível a realização de transações eletrônicas seguras e a troca de informações sensíveis e classificadas.

§ 2º A tecnologia de Chaves Públicas da ICP-Gov viabilizará, no âmbito dos órgãos e das entidades da Administração Pública Federal, a oferta de serviços de sigilo, a validade, a autenticidade e integridade de dados, a irrevogabilidade e irretratabilidade das transações eletrônicas e das aplicações de suporte que utilizem certificados digitais.

Art. 3º A ICP-Gov deverá contemplar, dentre outros, o conjunto de regras e políticas a serem definidas pela Autoridade de Gerência de Políticas - AGP, que visem estabelecer padrões técnicos, operacionais e de segurança para os vários processos das Autoridades Certificadoras - AC, integrantes da ICP-Gov.

Art. 4º Para garantir o cumprimento das regras da ICP-Gov, serão instituídos processos de auditoria, que verifiquem as relações entre os requisitos operacionais determinados pelas características dos certificados e os procedimentos operacionais adotados pelas autoridades dela integrantes.

Parágrafo único. Além dos padrões técnicos, operacionais e de segurança, a ICP-Gov definirá os tipos de certificados que podem ser gerados pelas AC.

CAPÍTULO II DA ORGANIZAÇÃO DA ICP-Gov

Art. 5º A arquitetura da ICP-Gov encontra-se definida no Anexo I a este Decreto.

Art. 6º À Autoridade de Gerência de Políticas - AGP, integrante da ICP-Gov, compete:

I - propor a criação da Autoridade Certificadora Raiz - AC Raiz;

II - estabelecer e administrar as políticas a serem seguidas pelas AC;

III - aprovar acordo de certificação cruzada e mapeamento de políticas entre a ICP-Gov e outras ICP externas;

IV - estabelecer critérios para credenciamento das AC e das Autoridades de Registro - AR;

V - definir a periodicidade de auditoria nas AC e AR e as sanções pelo descumprimento de normas por ela estabelecidas;

VI - definir regras operacionais e normas relativas a:

a) Autoridade Certificadora - AC;

b) Autoridade de Registro - AR;

c) assinatura digital;

d) segurança criptográfica;

e) repositório de certificados;

f) revogação de certificados;

g) cópia de segurança e recuperação de chaves;

h) atualização automática de chaves;

- i) histórico de chaves;
- j) certificação cruzada;
- l) suporte a sistema para garantia de irretratabilidade de transações ou de operações eletrônicas;
- m) período de validade de certificado;
- n) aplicações cliente;

VII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Gov, em especial da Política de Certificados - PC e das Práticas e Regras de Operação da Autoridade Certificadora, de modo a garantir:

- a) atendimento às necessidades dos órgãos e das entidades da Administração Pública Federal;
- b) conformidade com as políticas de segurança definidas pelo órgão executor da ICP-Gov; e
- c) atualização tecnológica.

Art. 7º Para assegurar a manutenção do grau de confiança estabelecido para a ICP-Gov, as AC e AR deverão credenciar-se junto a AGP, de acordo com as normas e os critérios por esta autoridade estabelecidos.

Art. 8º Cabe à AC Raiz a emissão e manutenção dos certificados das AC de órgãos e entidades da Administração Pública Federal e das AC privadas credenciadas, bem como o gerenciamento da Lista de Certificados Revogados - LCR.

Parágrafo único. Poderão ser instituídos níveis diferenciados de credenciamento para as AC, de conformidade com a sua finalidade.

Art. 9º As AC devem prestar os seguintes serviços básicos:

- I - emissão de certificados;
- II - revogação de certificados;
- III - renovação de certificados;
- IV - publicação de certificados em diretório;

V - emissão de Lista de Certificados Revogados - LCR;

VI - publicação de LCR em diretório; e

VII - gerência de chaves criptográficas.

Parágrafo único. A disponibilização de certificados emitidos e de LCR atualizada será proporcionada mediante uso de diretório seguro e de fácil acesso.

Art. 10. Cabe às AR:

I - receber as requisições de certificação ou revogação de certificado por usuários, confirmar a identidade destes usuários e a validade de sua requisição e encaminhar esses documentos à AC responsável;

II - entregar os certificados assinados pela AC aos seus respectivos solicitantes.

CAPÍTULO III DO MODELO OPERACIONAL

Art. 11. A emissão de certificados será precedida de processo de identificação do usuário, segundo critérios e métodos variados, conforme o tipo ou em função do maior ou menor grau de sua complexidade.

Art. 12. No processo de credenciamento das AC, deverão ser utilizados, além de critérios estabelecidos pela AGP e de padrões técnicos internacionalmente reconhecidos, aspectos adicionais relacionados a:

I - plano de contingência;

II - política e plano de segurança física, lógica e humana;

III - análise de riscos;

IV - capacidade financeira da proponente;

V - reputação e grau de confiabilidade da proponente e de seus gerentes;

VI - antecedentes e histórico no mercado; e

VII - níveis de proteção aos usuários dos seus certificados, em termos de cobertura jurídica e seguro contra danos.

Parágrafo único. O disposto nos incisos IV a VII não se aplica aos credenciamentos de AC Públicas.

Art. 13. Obedecidas às especificações da AGP, os órgãos e as entidades da Administração Pública Federal poderão implantar sua própria ICP ou ofertar serviços de ICP integrados à ICP-Gov.

Art. 14. A AC Privada, para prestar serviço à Administração Pública Federal, deve observar as mesmas diretrizes da AC Governamental, salvo outras exigências que vierem a ser fixadas pela AGP.

CAPÍTULO IV DA POLÍTICA DE CERTIFICAÇÃO

Art. 15. Serão definidos tipos de certificados, no âmbito da ICP-Gov, que atendam às necessidades gerais da maioria das aplicações, de forma a viabilizar a interoperabilidade entre ambientes computacionais distintos, dentro da Administração Pública Federal.

§ 1º Serão criados certificados de assinatura digital e de sigilo, atribuindo-se-lhes os seguintes níveis de segurança, consoante o processo envolvido:

I - ultra-secretos;

II - secretos;

III - confidenciais;

IV - reservados; e

V - ostensivos.

§ 2º Os certificados, além de outros que a AGP poderá estabelecer, terão uso para:

I - assinatura digital de documentos eletrônicos;

II - assinatura de mensagem de correio eletrônico;

III - autenticação para acesso a sistemas eletrônicos; e

IV - troca de chaves para estabelecimento de sessão criptografada.

Art. 16. À AGP compete tomar as providências necessárias para que os documentos, dados e registros armazenados e transmitidos por meio eletrônico, óptico, magnético ou similar passem a ter a mesma validade, reconhecimento e autenticidade que se dá a seus equivalentes originais em papel.

CAPÍTULO V DAS DISPOSIÇÕES FINAIS

Art. 17. Para instituição da ICP-Gov, deverá ser efetuado levantamento das demandas existentes nos órgãos governamentais quanto aos serviços típicos derivados da tecnologia de Chaves Públicas, tais como, autenticação, sigilo, integridade de dados e irretratibilidade das transações eletrônicas.

Art. 18. O Glossário constante do Anexo II apresenta o significado dos termos e siglas em português, que são utilizados no sistema de Chaves Públicas.

Art. 19. Compete ao Comitê Gestor de Segurança da Informação a concepção, a especificação e a coordenação da implementação da ICP-Gov, conforme disposto no art. 4º, inciso XIV, do Decreto nº 3.505, de 13 de junho de 2000.

Art. 20. Fica estabelecido o prazo de cento e vinte dias, contados a partir da data de publicação deste Decreto, para especificação, divulgação e início da implementação da ICP-Gov.

Art. 21. Implementados os procedimentos para a certificação digital de que trata este Decreto, a Casa Civil da Presidência da República estabelecerá cronograma com vistas à substituição progressiva do recebimento de documentos físicos por meios eletrônicos.

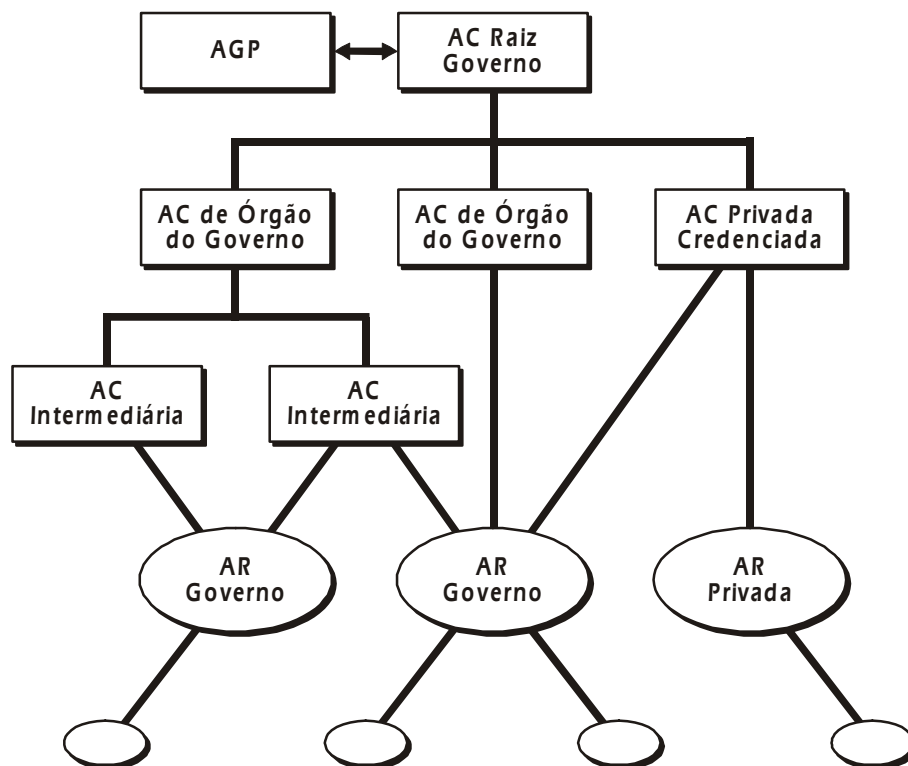
Art. 22. Este Decreto entra em vigor na data de sua publicação.

Brasília, 5 de setembro de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO

Guilherme Gomes Dias
Alberto Mendes Cardoso

Publicado no D.O. de 6.9.2000

ANEXO I
Arquitetura da ICP-Gov

ANEXO II - Glossário

Autenticação Authentication	Processo utilizado para confirmar a identidade de uma pessoa ou entidade, ou para garantir a fonte de uma mensagem.
Autoridade Certificadora -AC Certification Authority - CA	Entidade que emite certificados de acordo com as práticas definidas na Declaração de Regras Operacionais - DRO. É comumente conhecida por sua abreviatura - AC.
Autoridade Registradora - AR Registration Authority - RA	Entidade de registro. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota. É parte integrante de uma AC.
Assinatura Digital Digital Signature	Transformação matemática de uma mensagem por meio da utilização de uma função matemática e da criptografia assimétrica do resultado desta com a chave privada da entidade assinante.
Autorização Authorization	Obtenção de direitos, incluindo a habilidade de acessar uma informação específica ou recurso de uma maneira específica.
Chave Privada Private Key	Chave de um par de chaves mantida secreta pelo seu dono e usada no sentido de criar assinaturas para cifrar e decifrar mensagens com as Chaves Públicas correspondentes.
Certificado de Chave Pública Certificate	Declaração assinada digitalmente por uma AC, contendo, no mínimo: a) o nome distinto (DN - Distinguished Name) de uma AC, que emitiu o certificado; b) o nome distinto de um assinante para quem o certificado foi emitido; c) a Chave Pública do assinante; d) o período de validade operacional do certificado; e) o número de série do certificado, único dentro da AC; f) e uma assinatura digital da AC que emitiu o certificado com todas as informações citadas acima.
Chave Pública Public Key	Chave de um par de chaves criptográficas que é divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens.
Cifração Encryption	Processo de transformação de um texto original ("plaintext") em uma forma incompreensível ("ciphertext") usando um algoritmo criptográfico e uma chave criptográfica.

Credenciamento Accreditation	Processo de aprovação de políticas e procedimentos de uma AC, de forma que a mesma seja autorizada a participar de uma ICP.
Criptografia Cryptography	Disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo.
Criptografia de Chave Pública Public Key Cryptography	Tipo de criptografia que usa um par de chaves criptográficas matematicamente relacionadas. As Chaves Públicas podem ficar disponíveis para qualquer um que queira cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente. A chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.
Declaração de Regras Operacionais - DRO Certification Practice Statement - CPS	Documento que contém as práticas e atividades que uma AC implementa para emitir certificados. É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.
Emissão de Certificado Certificate Issuance	Emissão de um certificado por uma AC após a validação de seus dados, com a subsequente notificação do requerente sobre o conteúdo do certificado.
Gerenciamento de Certificado Certificate Management	Ações tomadas por uma AC, baseadas na sua DRO após a emissão do certificado, como armazenamento, disseminação e a subsequente notificação, publicação e renovação do certificado. Uma AC considera certificados emitidos e aceitos como válidos a partir da sua publicação.
Integridade de Mensagem Message Integrity	Garantia de que a mensagem não foi alterada durante a sua transferência, do emissor da mensagem para o seu receptor.
Irretratibilidade Nonrepudiation	Garantia de que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gerar.

Lista de Certificados Revogados - LCR Certification Revogation List - CRL	Lista dos números seriais dos certificados revogados, que é digitalmente assinada e publicada em um repositório. A lista contém ainda a data da emissão do certificado revogado e outras informações, tais como as razões específicas para a sua revogação.
Mensagem Message	Registro contendo uma representação digital da informação, como um dado criado, enviado, recebido e guardado em forma eletrônica.
Par de Chaves Key Pair	Chaves privada e pública de um sistema criptográfico assimétrico. A Chave Privada e sua Chave Pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da Chave Privada a partir da Chave Pública conhecida. A Chave Pública pode ser usada para verificação de uma assinatura digital que a Chave Privada correspondente tenha criado ou a Chave Privada pode decifrar a uma mensagem cifrada a partir da sua correspondente Chave Pública.
Política de Certificação - PC Certificate Police - CP	Documento que estabelece o nível de segurança de um determinado certificado
Raiz Root	Primeira AC em uma cadeia de certificação, cujo certificado é auto-assinado, podendo ser verificado por meio de mecanismos e procedimentos específicos, sem vínculos com este.
Registro Record	Informação registrada em um meio tangível (um documento) ou armazenada em um meio eletrônico ou qualquer outro meio perceptível.
Repositório Repository	Sistema confiável e acessível "on-line" para guardar e recuperar certificados e informações relacionadas com certificados.
Revogação de Certificado Certificate Revogation	Encerramento do período operacional de um certificado, podendo ser, sob determinadas circunstâncias, implementado antes do período operacional anteriormente definido.
Sigilo Confidentiality	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas.
Sistema Criptográfico Assimétrico Asymmetric Cryptosystem	Sistema que gera e usa um par de chaves seguras, consistindo de uma chave privada para a criação de assinaturas digitais ou decodificar de mensagens criptografadas e uma Chave Pública para verificação de assinaturas digitais ou de mensagens codificadas.

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

- I - Ministério da Justiça;
- II - Ministério da Fazenda;
- III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
- IV - Ministério do Planejamento, Orçamento e Gestão;
- V - Ministério da Ciência e Tecnologia;
- VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO

José Gregori

Martus Tavares

Ronaldo Mota Sardenberg

Pedro Parente

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001.

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea “a”, da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1º, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2º serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 4º Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º Este Decreto entra em vigor na data de sua publicação.

Art. 6º Fica revogado o Decreto nº 3.587, de 5 de setembro de 2000.

Brasília, 31 de outubro de 2001; 180º da Independência e 113º da República.

MARCO ANTONIO DE OLIVEIRA MACIEL

Martus Tavares

Silvano Gianni

RETIFICAÇÃO - DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

(Publicado no Diário Oficial da União de 5 de novembro de 2001, Seção 1, página 2)

No art. 2:

onde se lê: “Somente mediante prévia autorização do Comitê Gestor do Governo Eletrônico, ...”

leia-se: “Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, ..”

TRIBUNAL DE CONTAS DA UNIÃO

SAFS Quadra 4 Lote 1
70.042-900 - Brasília-DF
<http://www.tcu.gov.br>

RESPONSABILIDADE EDITORIAL

Secretaria Adjunta de Fiscalização

SAFS Quadra 4, Lote 1, Edifício Anexo I, Sala 404
70.042-900 - Brasília-DF
adfis@tcu.gov.br

Secretário-Geral de Controle Externo

Luciano Carlos Batista

Secretário Adjunto de Fiscalização

Cláudio Souza Castello Branco

Diretores da Diretoria de Auditoria da Tecnologia da Informação

Daniel Dias Pereira

André Luiz Furtado Pacheco

Elaboração

Cláudia Augusto Dias e
Roberta Ribeiro de Queiroz Martins

Revisão Técnica

André Luiz Furtado Pacheco

EDITORIAÇÃO

ISC

Instituto Serzedello Corrêa
Centro de Documentação
SAFS Quadra 4, Lote 1, Edifício-Sede, Sala 56
70.760-527 - Brasília-DF
isc_cedoc@tcu.gov.br

Instituto Serzedello Corrêa
Paulo Roberto Wiechers Martins

Centro de Documentação
Evelise Quadrado de Moraes

Serviço de Editoração e Publicações
Marcello Augusto Cardoso dos Santos

Revisão
Marília de Moraes Vasconcelos

ISC/CEDOC
 SEDIP

Esta obra foi composta no formato 190x210mm em Eras Light, Normal e Bold e impressa no sistema offset sobre papel couchê fosco 90g/m², com capa em papel couchê fosco 250g/m², pelo Serviço de Editoração e Publicações do Instituto Serzedello Corrêa para o Tribunal de Contas da União.

Brasília, 2003