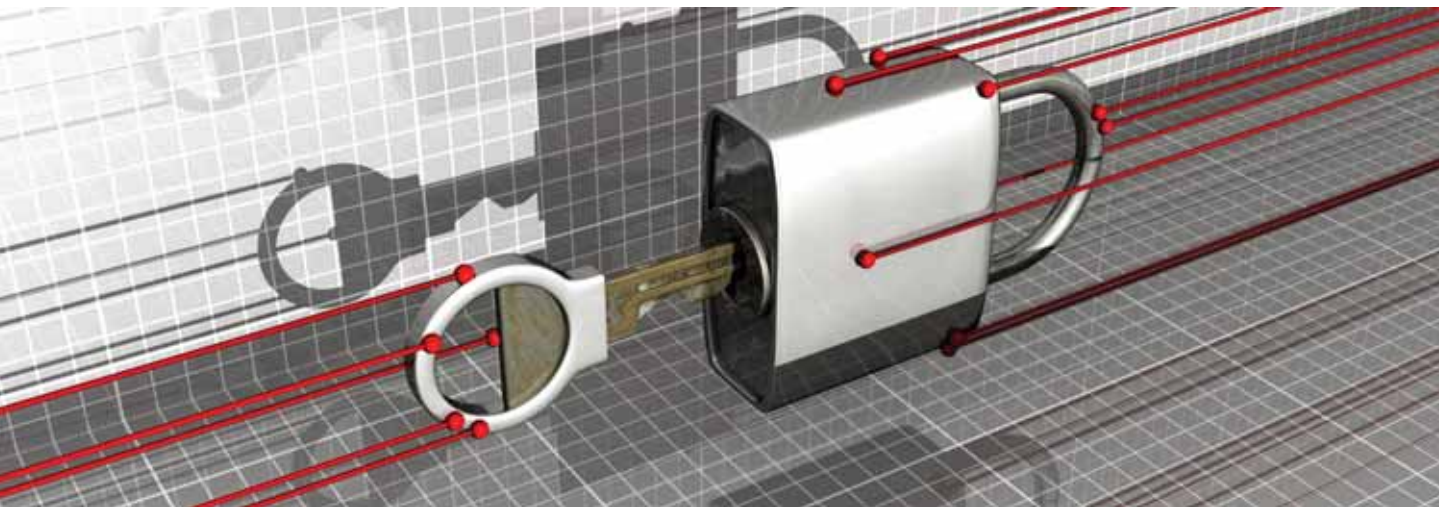


BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO



3ª EDIÇÃO

TRIBUNAL DE CONTAS DA UNIÃO 



República Federativa do Brasil
Tribunal de Contas da União

Ministros

Walton Alencar Rodrigues, Presidente
Ubiratan Aguiar, Vice-Presidente
Marcos Vinícios Vilaça
Valmir Campelo
Guilherme Palmeira
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro

Auditores

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho

Ministério Público

Lucas Rocha Furtado, Procurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Maria Alzira Ferreira, Subprocuradora-Geral
Marinus Eduardo de Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora
Júlio Marcelo de Oliveira, Procurador
Sérgio Ricardo Costa Caribé, Procurador

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



TRIBUNAL DE CONTAS DA UNIÃO

BOAS PRÁTICAS EM

SEGURANÇA DA INFORMAÇÃO

3ª EDIÇÃO

Brasília, 2008

© Copyright 2008, Tribunal de Contas da União

Impresso no Brasil / Printed in Brazil

<www.tcu.gov.br>

É permitida a reprodução desta publicação,
em parte ou no todo, sem alteração do conteúdo,
desde que citada a fonte e sem fins comerciais.

Brasil. Tribunal de Contas da União.

Boas práticas em segurança da informação / Tribunal de Contas da União. – 3. ed. – Brasília :
TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

70 p.

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

Apresentação

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

Um dos focos das fiscalizações de Tecnologia da Informação (TI), realizadas pela Secretaria de Fiscalização de Tecnologia da Informação (Sefti), do Tribunal de Contas da União, é a verificação da conformidade e do desempenho das ações governamentais em aspectos de segurança de tecnologia da informação, utilizando critérios fundamentados. O principal objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão pública, para assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

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, aos parlamentares, aos órgãos governamentais, à sociedade civil e às organizações não-governamentais, elaborou esta publicação com o intuito de despertar a atenção para os aspectos da segurança de tecnologia da informação nas organizações governamentais.

Espera-se que este trabalho seja uma boa fonte de consulta, e que o Tribunal, mais uma vez, colabore para o aperfeiçoamento da Administração Pública.

Walton Alencar Rodrigues
Ministro-Presidente

Sumário

Introdução7

Controles de Acesso Lógico9

Política de Segurança de Informações25

Plano de Contingências33

TCU e a NBR ISO/IEC 1779939

Introdução

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 com o uso de computadores de grande porte, a estrutura de segurança 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 de 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 segunda edição inclui um novo capítulo, que comenta a NBR ISO/IEC 17799 e lista acordãos e decisões do Tribunal sobre segurança de tecnologia da informação, além dos três capítulos que constavam da primeira edição (controles de acesso lógico, política de segurança de informações e plano de contingências). É nossa intenção continuar a publicar novas edições, incluindo capítulos sobre assuntos correlatos.

Diretoria de Auditoria de Tecnologia da Informação

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 por 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 por meio de um identificador de usuário (ID) e por 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 de 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 de 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 seis 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 de 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 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 sessenta, noventa dias é considerada 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 a 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 imediatamente no primeiro logon. 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 de 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 criptografados 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 de desligamentos de funcionários. 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. Atingido 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, de 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, a 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 essas, 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 de 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 o próprio 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 como as impressões digitais, em função dos erros causados por ruídos do ambiente e de 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 pela 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 de 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, por meio de autorização para uso de funções específicas ou para 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 (Access Control List (ACL)).

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, pelos 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 de 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 das 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 informação 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 por 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.

1.11 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.

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 pelos 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 gerência 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 genéricas e

amplios, 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 ter 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 de junho de 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 promovam 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 disponibilidade dos dados de interesse para a defesa nacional.

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 aplica-se 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 informações armazenadas em meio eletrônico, o que fazer na ocorrência de situações inesperadas que comprometam o processamento ou a 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 de 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 se restringem 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.

4. TCU e a NBR ISO/IEC 17799

Neste capítulo será comentada a norma NBR ISO/IEC 17799 como ferramenta de auditoria de segurança da informação utilizada pelo Tribunal de Contas da União (TCU). A fim de facilitar as atividades, tanto de gestão quanto de auditoria de segurança da informação, serão explanadas as seções da norma e citados acórdãos e decisões do Tribunal que tratam, entre outros aspectos, de segurança da informação.

4.1 De que trata a NBR ISO/IEC 17799?

A NBR ISO/IEC 17799, norma da Associação Brasileira de Normas Técnicas (ABNT), trata de técnicas de segurança em Tecnologia da Informação, e funciona como um código de prática para a gestão da segurança da informação. Essa norma foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados,

pela Comissão de Estudo de Segurança Física em Instalações de Informática, e é equivalente à norma ISO/IEC 17799.

4.2 Por que o TCU utiliza essa norma como padrão em suas auditorias de segurança da informação?

Além do reconhecimento da ABNT, como instituição normalizadora brasileira, as instituições internacionais ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), autoras da norma, são mundialmente reconhecidas por sua capacitação técnica. A norma ISO/IEC 17799, equivalente à norma brasileira, é amplamente reconhecida e utilizada por Entidades Fiscalizadoras Superiores, órgãos de governo, empresas públicas e privadas nacionais e internacionais atentas ao tema Segurança da Informação.

Os objetivos definidos nessa norma provêm diretrizes gerais sobre as práticas geralmente aceitas para a gestão da segurança da informação. Apesar de não ter força de lei, a NBR ISO/IEC 17799 configura-se como a melhor ferramenta de auditoria de segurança da informação disponível até a data de publicação deste Capítulo. Em seus acórdãos e decisões, o Tribunal já mencionou duas versões dessa norma: a mais recente, de 2005, e a anterior, de 2001.

4.3 Como está estruturada a NBR ISO/IEC 17799?

A NBR ISO/IEC 17799, versão 2005, está dividida em 11 seções:

- a) Política de segurança da informação;
- b) Organizando a segurança da informação;
- c) Gestão de ativos;
- d) Segurança em recursos humanos;
- e) Segurança física e do ambiente;
- f) Gestão das operações e comunicações;
- g) Controle de acessos;
- h) Aquisição, desenvolvimento e manutenção de sistemas de informação;
- i) Gestão de incidentes de segurança da informação;

- j) Gestão da continuidade do negócio;
- k) Conformidade.

4.4 De que trata a seção “Política de segurança da informação”?

Essa seção orienta a direção no estabelecimento de uma política clara de segurança da informação, alinhada com os objetivos do negócio, com demonstração de seu apoio e comprometimento com a segurança da informação por meio da publicação, manutenção e divulgação da política para toda a organização. São fornecidas diretrizes para elaboração do documento e sua análise crítica.

4.5 Que acórdãos e decisões do TCU tratam, entre outros aspectos, de “Política de segurança da informação”?

Acórdão 1092/2007 - Plenário

9.1.2. elabore, aprove e divulgue Política de Segurança da Informação - PSI conforme o estabelecido na NBR ISO/IEC 17799:2005, item 5.1.1;

9.1.4. crie mecanismos para que as políticas e normas de segurança da informação se tornem conhecidas, acessíveis e observadas por todos os funcionários e colaboradores da Empresa conforme o estabelecido na NBR ISO/IEC 17799:2005, item 5.1.1;

Acórdão 71/2007 - Plenário

9.2.6. defina formalmente uma Política de Segurança da Informação - PSI - para o Infoseg, que forneça orientação e apoio para a segurança da informação da rede, promovendo-se ampla divulgação do documento para todos os usuários, de acordo com o previsto no item 5.1.1 da NBR ISO/IEC 17799:2005;

9.2.10. crie mecanismos para que as políticas e normas se tornem conhecidas, acessíveis e observadas por todos os usuários e gestores do Infoseg, de acordo com o previsto no item 5.1.1 da NBR ISO/IEC 17799:2005;

Acórdão 562/2006 - Plenário

9.2.1. desenvolva Plano de Tecnologia da Informação para ser utilizado no âmbito do Sistema Nacional de Transplantes (SNT) que contemple [...] o atendimento aos princípios de segurança da informação, preconizados no item 3.1 da Norma NBR ISO/IEC 17799:2001;

Acórdão 2023/2005 - Plenário

9.1.2. defina uma Política de Segurança da Informação, nos termos das orientações contidas no item 3 da NBR ISO/IEC 17799:2001, que estabeleça os princípios norteadores da gestão da segurança da informação no Ministério e que esteja integrada à visão, à missão, ao negócio e às metas institucionais, observando a regulamentação ou as recomendações porventura feitas pelo Comitê Gestor de Segurança da Informação instituído

pelo Decreto nº 3.505/2000 e pelo Gabinete de Segurança Institucional da Presidência da República, conforme Decreto n. 5.408, de 1º/04/2005;

9.1.6. crie mecanismos para que as políticas e normas se tornem conhecidas, acessíveis e observadas por todos os servidores e prestadores de serviços do Ministério;

Acórdão 782/2004 – 1ª Câmara

9.4. [...] formalizem a política de segurança de informação do sistema informatizado de pagamento de pessoal [...];

Acórdão 461/2004 - Plenário

9.1.1. a concepção e implementação de uma política de segurança de informações formal e, preferencialmente, baseada nos ditames da norma NBR ISO/IEC 17799;

Decisão 38/2003 - Plenário

9.2 d) promova a aprovação de sua política de segurança da informação.

Decisão 595/2002 - Plenário

8.1.23 b) elaborar e implantar política de segurança de informações, com abrangência nacional e vinculando os prestadores de serviços, prevendo um programa de conscientização dos usuários a respeito das responsabilidades inerentes ao acesso às informações e à utilização

dos recursos de TI, reavaliando as situações existentes, especialmente no tocante à segurança lógica e física;

Decisão 918/2000 - Plenário

8.2.6.3. definir e implementar política formal de segurança lógica, consoante as diretrizes previstas no Projeto BRA/97-024, de cooperação técnica, [...] incluindo ações e procedimentos para disseminar a importância da segurança da informação para os funcionários da unidade, e estabelecer segregação de funções dentro do ambiente de informática, notadamente entre desenvolvimento, produção e administração de segurança lógica;

4.6 De que trata a seção “Organizando a segurança da informação”?

Essa seção da norma orienta a direção de como gerenciar a segurança da informação dentro da organização e, ainda, de como manter a segurança de seus recursos de processamento da informação, que são acessados, processados, comunicados ou gerenciados por partes externas.

São fornecidas diretrizes para definição de infraestrutura de segurança da informação, detalhando os itens: comprometimento da gerência, coordenação, atribuição de responsabilidades, processo de autorização para recursos de processamento da informação, acordos de confidencialidade, análise crítica independente, contato com autoridades e grupos de interesses

especiais. São fornecidas ainda diretrizes para o relacionamento com partes externas, na identificação dos riscos relacionados e dos requisitos de segurança da informação necessários ao tratar com clientes e terceiros.

4.7 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Organização da segurança da informação”?

Infra-estrutura da segurança da informação

Acórdão 1092/2007 - Plenário

9.1.1. estabeleça responsabilidades internas quanto à segurança da informação conforme o estabelecido na NBR ISO/IEC 17799:2005, item 6.1.3;

Acórdão 71/2007 - Plenário

9.2.5. estabeleça e identifique formalmente responsabilidades relativas às questões de segurança das informações do Infoseg, de acordo com o previsto no item 6.1.3 da NBR ISO/IEC 17799:2005;

Acórdão 2023/2005 - Plenário

9.1.1. estabeleça institucionalmente as atribuições relativas à segurança da informação, conforme preceituam os itens 4.1.1, 4.1.2 e 4.1.3 da NBR ISO/IEC 17779:2001 e o item PO4.6 do Cobit;

9.1.13.6. obrigatoriedade de assinatura de Termo de Compromisso ou Acordo de Confidencialidade por parte dos prestadores de serviços, contendo declarações que permitam aferir que os mesmos tomaram ciência das normas de segurança vigentes no órgão;

Acórdão 782/2004 - 1ª Câmara

9.3.1. envide esforços para proceder à redefinição do regimento interno da unidade, de modo que fiquem claramente explicitadas suas atribuições, responsabilidades e poderes como gestor de segurança do sistema informatizado de pagamento de pessoal [...];

Acórdão 461/2004 - Plenário

9.1.8. estudos com vistas à criação de uma gerência específica de segurança, preferencialmente vinculada à direção geral;

Decisão 1049/2000 - Plenário

8.1.7. estude a possibilidade de criação de um grupo de controle/segurança, na área de informática, que seja responsável por:

- a) investigar e corrigir qualquer problema operacional em terminal, microcomputador ou outro dispositivo de entrada de dados;
- b) investigar qualquer ação de intervenção do operador;

c) assegurar que os procedimentos de “restart” sejam executados de maneira correta;

d) monitorar as atividades de entrada de dados no terminal, microcomputador ou outro dispositivo similar; e

e) investigar qualquer desvio dos procedimentos de entrada de dados pré-estabelecidos;

8.3.3. quando de sua reestruturação organizacional, atente para o posicionamento hierárquico da área de segurança física e lógica de sistemas, que deve constar em um nível superior, de forma a conter todas as funções de segurança delineadas como necessárias, estabelecendo, em consequência, segregação na execução das mesmas;

Decisão 918/2000 - Plenário

8.2.6.2. realizar estudos com o objetivo de instituir setor ou gerência específica para segurança lógica na unidade;

Partes externas

Acórdão 71/2007 - Plenário

9.2.21. formalize, junto à Agência Estadual de Tecnologia da Informação do Estado de Pernambuco - ATI -, um termo de compromisso que contemple de maneira específica a cópia das bases de dados do Infoseg que se encontra naquelas instalações, estabelecendo nele cláusulas

de sigilo e responsabilização pelo uso indevido dos equipamentos ou divulgação não autorizada dos dados;

9.4. [...] defina claramente, tanto nos editais de licitação como nos contratos, cláusulas contemplando requisitos de segurança da informação como os previstos no item 6.2.3 da NBR ISO/IEC 17799:2005;

Acórdão 1663/2006 - Plenário

9.2.3. elabore o acordo de nível de serviço do Sípia;

Acórdão 914/2006 - Plenário

9.1.1. firmem contrato com relação ao Programa do Fundo de Financiamento ao Estudante do Ensino Superior (Fies), devendo ser estabelecida nesse instrumento cláusula que disponha sobre a propriedade intelectual de programas, documentação técnica e dados do Sistema do Financiamento Estudantil (Sifes);

9.3.1. firmem Acordo de Nível de Serviço, ou documento correlato, em relação ao Sifes, contemplando as áreas envolvidas, em especial a de desenvolvimento do sistema, com o objetivo de estabelecer entendimento comum sobre a natureza dos serviços propostos e os critérios de medição de desempenho, devendo este acordo considerar elementos tais como:

9.3.1.1. participantes do acordo, funções e responsabilidades;

9.3.1.2. descrição detalhada dos serviços que serão prestados;

9.3.1.3. níveis de serviços desejados e respectivos critérios de medição e indicadores, em termos de disponibilidade, confiabilidade, tempo de resposta, atendimento ao usuário (help-desk), capacidade de crescimento, prazos para solicitação e atendimento de demandas (inclusive emergenciais), testes, homologação, segurança e outros que as partes julgarem necessários;

9.3.1.4. responsável pela medição dos serviços;

9.3.1.5. ações a serem tomadas quando da ocorrência de problemas na prestação dos serviços (ações corretivas, penalidades e outras);

Acórdão 2085/2005 - Plenário

9.4.3. faça prever nos contratos de terceirização de serviços de desenvolvimento de software o repasse da respectiva tecnologia, incluindo toda a documentação do produto desenvolvido, com o intuito de se evitar a futura dependência do suporte e da manutenção desse produto, o que elevaria os custos da terceirização dessa atividade, bem como impedir que terceiros tenham acesso irrestrito aos sistemas desenvolvidos;

Acórdão 2023/2005 - Plenário

9.1.13. inclua os seguintes requisitos de segurança em contratos de prestação de serviços e locação de mão-de-obra em Tecnologia da Informação que vierem a ser celebrados a partir da presente data, em atenção aos itens 4.2.2 e 4.3.1 da NBR ISO/IEC 17799:2001:

9.1.13.1. obrigatoriedade de aderência à Política de Segurança da Informação, à Política de Controle de Acesso, à Metodologia de Desenvolvimento de Sistemas e às outras normas de segurança da informação vigentes no Ministério;

9.1.13.2. Acordo de Nível de Serviço, negociado entre os grupos de usuários e o fornecedor dos serviços, com o objetivo de estabelecer um entendimento comum da natureza dos serviços propostos e critérios de medição de desempenho, que deverá conter, no mínimo, os seguintes elementos: participantes do acordo; descrição clara dos serviços e funcionalidades disponíveis, para contratos de prestação de serviços; descrição clara dos perfis profissionais desejados, para contratos de locação de mão-de-obra; funções e responsabilidades; níveis de serviços desejados em termos de disponibilidade, prazos, desempenho, segurança, quantidade, qualidade e outros; indicadores de níveis de serviços; responsável pela medição dos serviços; ações a serem tomadas quando da ocorrência de problemas de mau desempenho (ações corretivas, penalidades financeiras e outras);

9.1.13.3. definição clara acerca da propriedade dos dados entregues pela Administração Pública a empresas contratadas, coletados por essas empresas em nome da Administração Pública ou produzidos por programas de computadores decorrentes de contratos de prestação de serviços;

9.1.13.4. definição acerca dos direitos de propriedade de programas, de acordo com a Lei n. 9.609/1998, de documentação técnica e forma de acesso a eles; se o contrato dispuser que programas e documentação técnica não pertencem à Administração Pública, o projeto básico deve apresentar a justificativa de tal escolha; caso contrário, o contrato deve estabelecer de que forma e em que prazo se dará o acesso aos mesmos, inclusive na ocorrência de fatos imprevisíveis ou de força maior; recomenda-se que se estabeleça, como data limite para entrega de programas fontes e documentação, a data de homologação dos mesmos;

9.1.13.5. obrigatoriedade de manter sigilo sobre o conteúdo de programas de computadores (fontes e executáveis), documentação e bases de dados; deve ser estabelecido um período durante o qual subsistirão as obrigações de manter sigilo;

9.1.13.6. obrigatoriedade de assinatura de Termo de Compromisso ou Acordo de Confidencialidade por parte dos prestadores de serviços, contendo declarações que permitam aferir que os mesmos tomaram ciência das normas de segurança vigentes no órgão;

9.1.13.7. garantia do direito de auditar, por parte da contratada e dos órgãos de controle, e forma de exercício deste direito;

9.4.4. adote cláusulas contratuais para assegurar que a documentação técnica, programas fontes e dados de sistemas regidos por contratos de prestação de serviços estejam acessíveis ao Ministério;

Acórdão 441/2005 – 1ª Câmara

1.3 elabore o Acordo de Nível de Serviço do Sisfin;

1.4 inclua nas normas internas a obrigatoriedade da elaboração de Acordo de Nível de Serviço para os sistemas críticos;

Decisão 295/2002 - Plenário

8.1.1 - quanto aos sistemas informatizados:

a) revise os atuais critérios de habilitação de cadastradores do Sistema Integrado de Administração Patrimonial (SIAPA), sejam eles gerais, parciais ou locais, reavaliando a pertinência da existência de funcionários do Serviço Federal de Processamento de Dados (SERPRO) desempenhando esse papel;

f) revise os atuais critérios de habilitação de cadastradores do Sistema do Patrimônio Imobiliário da União (SPIU), sejam eles gerais, parciais ou locais, lotados na SPU ou

não, reavaliando, entre outros aspectos, a pertinência da existência de funcionários de outros órgãos ou entidades, especialmente do SERPRO, que atualmente desempenham esse papel;

4.8 De que trata a seção “Gestão de ativos”?

Essa seção da norma orienta a direção a alcançar e manter a proteção adequada dos ativos da organização, além de assegurar que a informação seja classificada de acordo com seu nível adequado de proteção. São fornecidas diretrizes para realização de inventário dos ativos, definição de seus proprietários e regras para seu uso. Em relação à classificação da informação, a norma faz algumas recomendações e sugere a definição de procedimentos para rotulação e tratamento da informação.

4.9 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Gestão de ativos”?

Responsabilidade pelos ativos

Acórdão 1092/2007 - Plenário

9.1.3. inventarie os ativos de informação conforme o estabelecido na NBR ISO/IEC 17799:2005, itens 7.1.1 e 7.1.2, e estabeleça critérios para a classificação desses ativos conforme o estabelecido na NBR ISO/IEC 17799:2005, item 7.2;

Acórdão 71/2007 - Plenário

9.2.19. formalize o inventário dos ativos do Infoseg, em conformidade com o previsto no item 7.1.1 da NBR ISO/IEC 17799:2005;

9.2.20 defina formalmente o proprietário de cada ativo constante do inventário acima, em conformidade com o item 7.1.2 da NBR ISO/IEC 17799:2005, atentando para a assinatura das cautelas que se fizerem necessárias;

Acórdão 782/2004 - 1ª Câmara

9.3.2. adote providências para designar formalmente um membro [...] como gestor do sistema Siappes, e futuramente, do sistema Sispag;

9.3.5. formule [...] o inventário de ativos de informação, compreendendo a classificação do nível de confidencialidade de cada ativo e a definição de procedimentos para garantir a segurança nas diversas mídias nas quais a informação é armazenada ou pelas quais é transmitida, como o papel, as fitas magnéticas e as redes local e externa;

Decisão 1049/2000 - Plenário

8.4.1. adote medidas no sentido de viabilizar um controle efetivo dos equipamentos de hardware que compõem o parque computacional;

Classificação da informação

Acórdão 1092/2007 - Plenário

9.1.3. inventarie os ativos de informação conforme o estabelecido na NBR ISO/IEC 17799:2005, itens 7.1.1 e 7.1.2, e estabeleça critérios para a classificação desses ativos conforme o estabelecido na NBR ISO/IEC 17799:2005, item 7.2;

Acórdão 1832/2006 - Plenário

9.1.9 implemente critérios para a classificação e marcação de informações e documentos sigilosos;

9.2.11 - institua procedimento para atribuir grau de sigilo a todos os documentos que contenham, de algum modo, informações estratégicas e/ou privilegiadas, não importando a quem se destine, ou quem deterá a sua posse;

Acórdão 2023/2005 - Plenário

9.1.4. crie critérios de classificação das informações a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, a teor do disposto pelo item 5 da NBR ISO/IEC 17799:2001;

Acórdão 441/2005 – 1ª Câmara

1.5 implemente a indicação de classificação das informações apresentadas nas telas e relatórios dos novos sistemas que estão em desenvolvimento em substituição ao Sisfin;

Acórdão 782/2004 - 1ª Câmara

9.3.5. formule [...] o inventário de ativos de informação, compreendendo a classificação do nível de confidencialidade de cada ativo e a definição de procedimentos para garantir a segurança nas diversas mídias nas quais a informação é armazenada ou pelas quais é transmitida, como o papel, as fitas magnéticas e as redes local e externa;

Acórdão 461/2004 - Plenário

9.1.6. a classificação do nível de segurança e controle de acesso aos dados, no âmbito do Projeto “Repositório”;

Decisão 1098/2002 - Plenário

8.3 [...] coordene a elaboração de metodologia para classificação das informações, nos termos do item 5.2 da Norma ISO/IEC 17799:2001.

4.10 De que trata a seção “Segurança em recursos humanos”?

Essa seção da norma orienta a direção a assegurar que funcionários, fornecedores e terceiros compreendam suas responsabilidades, estejam

conscientes das ameaças relativas à segurança da informação e prontos para apoiar a política de segurança da informação da organização. São fornecidas diretrizes para definição de papéis e responsabilidades, inclusive da direção, seleção de pessoal, termos e condições de contratação, conscientização, educação e treinamento em segurança da informação, e processo disciplinar.

Para os casos de encerramento ou mudança da contratação, são fornecidas diretrizes para encerramento de atividades, devolução de ativos e retirada de direitos de acesso. Essa seção abrange contratação temporária ou de longa duração de pessoas, nomeação e mudança de funções, atribuição de contratos e encerramento de qualquer uma dessas situações.

4.11 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Segurança de recursos humanos”?

Acórdão 2023/2005 - Plenário

9.1.3.4. identificação dos responsáveis pela guarda dos termos de compromisso assinados, além do tempo mínimo de armazenamento desses documentos, conforme propõem os itens 6.1.4 e 6.3.5 da NBR ISO/IEC 17799:2001;

Acórdão 782/2004 - 1ª Câmara

9.2.1. adote procedimentos formais de concessão e de validação periódica de senhas de usuários de sistemas informatizados, bem como

de cancelamento de acesso de usuários que são desligados da unidade;

9.2.4. e 9.3.4. adote um programa de treinamento específico para a área de segurança de sistemas, enfocando aspectos de segurança física e lógica, bem assim a reação dos funcionários frente à ocorrência de contingências que possam afetar a continuidade dos serviços;

Decisão 1098/2002 - Plenário

8.2.6 automatização de procedimento de cancelamento de acessos e autorizações, no caso de mudança de situação do servidor;

Decisão 295/2002 - Plenário

8.1.1 - quanto aos sistemas informatizados:

b) reveja as habilitações de todos os usuários do SIAPA lotados na [...], reavaliando não apenas sua permanência na Secretaria, como também seu local de trabalho (gerência) e a pertinência dos níveis de acesso concedidos;

d) estabeleça controle sistemático e oriente as Gerências Regionais [...] quanto à necessidade de exclusão de usuários do SIAPA, no Senha-Rede, quando das suas saídas da [..];

h) reveja as habilitações de todos os usuários do SPIU, lotados na [...] ou não, reavaliando sua permanência no órgão e a pertinência dos níveis de acesso concedidos, assim como os inúmeros acessos concedidos a funcionários lotados no

SERPRO, inclusive pertencentes à equipe de manutenção do sistema;

Decisão 918/2000 – Plenário

8.1.1 adote ações específicas de orientação aos gestores locais, quanto aos aspectos de segurança do IH/SUS, elaborando, se necessário, normas e cartilhas para tal mister;

8.2.6.3. definir e implementar política formal de segurança lógica, consoante as diretrizes previstas no Projeto BRA/97-024, de cooperação técnica [...], incluindo ações e procedimentos para disseminar a importância da segurança da informação para os funcionários da unidade, e estabelecer segregação de funções dentro do ambiente de informática, notadamente entre desenvolvimento, produção e administração de segurança lógica;

4.12 De que trata a seção “Segurança física e do ambiente”?

Essa seção da norma orienta a direção a prevenir acesso físico não autorizado, danos e interferências nas instalações e informações, assim como a impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização. São fornecidas diretrizes para áreas seguras, incluindo perímetro de segurança física, controles de entrada física, segurança em escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do público, áreas de entrega e carregamento.

Para a segurança de equipamentos, são dadas recomendações para instalação e proteção de equipamento, inclusive contra falta de energia elétrica e outras interrupções provocadas por falhas das utilidades, segurança do cabeamento, manutenção de equipamentos, segurança de equipamentos fora das dependências da organização, reutilização e alienação segura de equipamentos, e, por fim, remoção de propriedade.

4.13 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Segurança física e do ambiente”?

Áreas seguras

Acórdão 71/2007 - Plenário

9.2.17. estabeleça um perímetro de segurança nas instalações da gerência do Infoseg (barreiras tais como paredes, portões de entrada controlados por cartão ou balcão com recepcionista), em conformidade com o item 9.1.1 da NBR ISO/IEC 17799:2005;

9.2.18. realize as obras necessárias de forma que se constituam barreiras físicas suficientes nas instalações da gerência do Infoseg que impeçam o acesso de pessoas não autorizadas, em conformidade com a diretriz “b” do item 9.1.1 da NBR ISO/IEC 17799:2005;

Acórdão 1832/2006 - Plenário

9.2.9 - implemente medidas no sentido de garantir maior segurança às informações relativas à dívida, notadamente no que tange ao acesso de pessoas estranhas ou não autorizadas aos diversos recintos envolvidos com a operação da dívida pública, até que o “Projeto de Segurança” seja definitivamente implantado;

Acórdão 2085/2005 - Plenário

9.4.1. não autorize o acesso de terceiros às áreas dos sistemas informatizados da empresa que possam possibilitar a execução de transações indevidas, de forma a evitar a sua exposição a um risco maior de fraudes;

Acórdão 782/2004 - 1ª Câmara

9.3.7. formalize um esquema de segurança especial para guarda e manipulação das fitas, com a criação de um ambiente de acesso restrito para o seu armazenamento, visando garantir que a informação nelas contida não seja consultada ou alterada indevidamente;

Decisão 918/2000 - Plenário

8.2.6.10. adotar procedimentos de segurança física efetivos para prevenir o acesso de pessoas não autorizadas ao ambiente de processamento de dados (CPD);

8.2.6.11. divulgar internamente os procedimentos de proteção contra incêndios e envidar esforços para instituir Comissão Interna de Prevenção de Acidentes (Cipa);

Decisão 445/1998 - Plenário

3.7.1. disciplinar de forma rígida o acesso de pessoas aos andares do prédio onde a Gerência Executiva de Tecnologia [...] se encontra instalada;

Segurança de equipamentos

Acórdão 2083/2005 – 2ª Câmara

9.3.13. adote medidas no sentido da instalação de “No Break” nos computadores da Empresa de modo a afastar o risco de perda de dados e avarias no software;

Acórdão 2023/2005 - Plenário

9.1.15. aprimore os controles de acesso físico aos computadores e equipamentos considerados críticos;

4.14 De que trata a seção “Gerenciamento das operações e comunicações”?

Essa seção da norma orienta a direção quanto aos procedimentos e responsabilidades operacionais, incluindo gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e teste. São

fornecidas diretrizes também para gerenciamento de serviços terceirizados, planejamento e aceitação de sistemas, proteção contra códigos maliciosos e móveis, cópias de segurança, gerenciamento da segurança em redes, manuseio de mídias, troca de informações, serviços de correio eletrônico e, por fim, monitoramento.

4.15 Que acórdãos e decisões do TCU tratam, entre outros aspectos, do “Gerenciamento das operações e comunicações”?

Procedimentos e responsabilidades operacionais

Acórdão 914/2006 - Plenário

9.5.3. providencie a implantação do Sifes em ambiente de homologação dedicado a essa finalidade;

Acórdão 562/2006 - Plenário

9.2.2. elabore e distribua a todas as CNCDOs manual de procedimentos, instruindo sobre operação e controle dos sistemas monousuários, que contemple pelo menos procedimentos detalhados para realização, guarda e restauração de cópias de segurança; orientação quanto ao uso de senhas por parte dos operadores do sistema; orientação quanto à segurança física dos equipamentos que efetuam o processamento do sistema; orientação quanto à utilização de software de proteção contra programas maliciosos (vírus); e elaboração de “plano de contingência” para o

sistema, de forma a evitar que, em eventuais falhas no seu funcionamento ou nos equipamentos, as listas de prováveis receptores deixem de ser emitidas;

Acórdão 2023/2005 - Plenário

9.1.14. o acesso ao ambiente de produção por técnicos da CGI seja feito de forma controlada pelos gestores dos sistemas;

9.4.8. não assuma responsabilidades inerentes às áreas de negócio, como a inserção, alteração e exclusão de informações em bases de dados;

9.4.9. evite executar procedimentos que envolvam alterações de informações diretamente na base de dados de produção, devendo as situações de exceção, depois de devidamente identificadas, ser implementadas dentro das funcionalidades dos respectivos sistemas, tornando-as disponíveis para serem utilizadas de forma segura pelos usuários desses sistemas;

9.4.11. crie procedimentos automatizados (preferencialmente um sistema) que permitam o acompanhamento detalhado das demandas de TI feitas pelas outras áreas do Ministério;

Acórdão 782/2004 - 1ª Câmara

9.3.3. adote providências para elaborar um esquema de segregação de funções e atividades, incluindo a separação dos ambientes de desenvolvimento, teste e produção, de modo a minimizar a possibilidade de ocorrência de fraudes

ocasionadas pelo fato de um mesmo usuário ser detentor de permissões para modificar o código fonte do sistema, inserir e consultar dados;

Decisão 1380/2002 - Plenário

8.3.4 defina procedimentos claros, escritos ou automatizados, que esclareçam os passos a serem adotados em caso de necessidade de reprocessamento de qualquer rotina batch;

Decisão 295/2002 – Plenário

8.1.1 - quanto aos sistemas informatizados:

c) proceda à reavaliação geral das pessoas habilitadas no SIAPA, particularmente com relação àquelas lotadas em outros órgãos/entidades, como o SERPRO;

h) reveja as habilitações de todos os usuários do SPIU, lotados na [...] ou não, reavaliando sua permanência no órgão e a pertinência dos níveis de acesso concedidos, assim como os inúmeros acessos concedidos a funcionários lotados no SERPRO, inclusive pertencentes à equipe de manutenção do sistema;

Decisão 1049/2000 – Plenário

8.3.16. estude a possibilidade de criar um pseudo-sistema dentro do Designer 2000 que permita o acesso somente à leitura da documentação pelas equipes de desenvolvimento, para que não se perca o controle sobre alterações efetuadas;

Decisão 918/2000 - Plenário

8.2.6.3. [...] estabelecer segregação de funções dentro do ambiente de informática, notadamente entre desenvolvimento, produção e administração de segurança lógica;

8.2.8. adote providências com vistas a exercer supervisão direta e efetiva das atividades de operação do CPD;

Planejamento e aceitação dos sistemas

Acórdão 71/2007 - Plenário

9.2.13. estabeleça critérios formais para homologação e aceitação de atualizações e novas versões do Infoseg, de acordo com o previsto no item 10.3.2 da NBR ISO/IEC 17799:2005;

Acórdão 1663/2006 - Plenário

9.1.4. implemente sistemática de homologação e controle das versões implantadas do Sipia;

Acórdão 914/2006 - Plenário

9.3.2. façam constar do contrato firmado entre ambos a exigência de etapa formal de homologação [...] das alterações implementadas no Sifes pelo agente operador;

9.5.1. realize adequadamente os testes e homologação do Sifes, mantendo a documentação dos procedimentos realizados;

Decisão 1049/2000 - Plenário

8.3.1. proceda a estudos objetivando a otimização da utilização de seus mainframes, incluindo projeções futuras dessa utilização, com vistas a evitar problemas no processamento de dados;

Proteção contra códigos maliciosos e códigos móveis

Decisão 918/2000 – Plenário

8.2.10.3. intensificar ações visando tornar mais eficientes os procedimentos de proteção antivírus dos seus microcomputadores, implementando, assim que possível, dispositivos para automatizar a atualização das versões de softwares antivírus nos equipamentos instalados, bem como divulgando internamente a necessidade de aplicar o programa antivírus sobre disquetes provenientes de outros equipamentos;

Cópias de segurança

Acórdão 71/2007 - Plenário

9.2.15. formalize política de geração de cópias de segurança para o Infoseg, de acordo com o previsto no item 10.5.1 da NBR ISO/IEC 17799:2005;

9.2.16. armazene as mídias contendo cópias de segurança do Infoseg em local diverso da operação do sistema, de acordo com a diretriz “d” do item 10.5.1 da NBR ISO/IEC 17799:2005;

Acórdão 1049/2000 – Plenário

8.3.13. adote providências com vistas a:

a) preservar as versões anteriores das estruturas de banco de dados, de forma a recompor emergencialmente situações anteriores;

Decisão 445/1998 - Plenário

3.7.2. definir, oficialmente, junto aos gestores responsáveis, uma sistemática de “back-up” para os sistemas existentes;

Gerenciamento da segurança em redes

Decisão 918/2000 - Plenário

8.2.10. adote providências para melhorar a eficiência e eficácia das ações/procedimentos referentes à gerência da sua rede de comunicação e de microcomputadores, sem prejuízo de:

8.2.10.1. realizar estudos com o fito de instituir setor ou gerência específica para rede na unidade, sem prejuízo de definir e implementar política formal de gerenciamento da rede, consoante as diretrizes previstas no Projeto BRA/97-024;

8.2.10.2. aprimorar o controle do processamento em rede, especialmente quanto à adoção de: testes e verificações sistemáticas dos procedimentos e recursos relativos ao processamento de rede; políticas e procedimentos específicos de auditoria

de rede; utilização de software adequado para gerência de rede; implementação, tão logo possível, de dispositivo tipo firewall para preservar a segurança da rede;

Decisão 445/1998 – Plenário

3.7.3. definir, com a maior brevidade possível, mecanismos de segurança na área de transmissão de dados;

Manuseio de mídias

Acórdão 1832/2006 - Plenário

9.1.4 estabeleça procedimento para controlar fisicamente o acesso de pessoas aos documentos;

9.1.10 estabeleça procedimento para controlar fisicamente e registrar o acesso de pessoas aos documentos que contenham informações estratégicas e/ou privilegiadas, que possam beneficiar terceiros;

9.2.12 adote procedimento especial para o registro e a tramitação de todos os documentos, que contenham, de algum modo, informações estratégicas e/ou privilegiadas;

Acórdão 2023/2005 - Plenário

9.4.2. crie e defina mecanismos de gerenciamento que garantam a guarda

e recuperação das versões atualizadas da documentação de sistemas pelo setor responsável;

Acórdão 782/2004 - 1ª Câmara

9.3.5. [...] definição de procedimentos para garantir a segurança nas diversas mídias nas quais a informação é armazenada ou pelas quais é transmitida, como o papel, as fitas magnéticas e as redes local e externa;

9.3.7. formalize um esquema de segurança especial para guarda e manipulação das fitas, com a criação de um ambiente de acesso restrito para o seu armazenamento, visando garantir que a informação nelas contida não seja consultada ou alterada indevidamente;

Decisão 1049/2000 - Plenário

8.3.16. estude a possibilidade de criar um pseudo-sistema dentro do Designer 2000 que permita o acesso somente à leitura da documentação pelas equipes de desenvolvimento, para que não se perca o controle sobre alterações efetuadas;

Decisão 918/2000 – Plenário

8.1.6. envide esforços para automatizar o controle de qualidade do processamento do SIH/SUS (conferência da regularidade do

processamento mensal), bem como o processo de disponibilização dos respectivos arquivos de saída na BBS/MS;

Decisão 445/1998 - Plenário

3.7.7. elaborar documentação completa dos sistemas que compõem o FGTS e mantê-la atualizada em ambientes de fácil acesso por quem for autorizado;

Troca de informações

Acórdão 1832/2006 - Plenário

9.2.12 - adote procedimento especial para o registro e a tramitação de todos os documentos, que contenham, de algum modo, informações estratégicas e/ou privilegiadas;

Acórdão 782/2004 - 1ª Câmara

9.3.5. [...] definição de procedimentos para garantir a segurança nas diversas mídias nas quais a informação é armazenada ou pelas quais é transmitida, como o papel, as fitas magnéticas e as redes local e externa;

Decisão 445/1998 - Plenário

3.7.3. definir, com a maior brevidade possível, mecanismos de segurança na área de transmissão de dados;

Monitoramento

Acórdão 71/2007 - Plenário

9.2.24. implemente controles compensatórios (autorização formal, registro e monitoramento das alterações) para as operações dos administradores de banco de dados do Infoseg de forma a permitir o registro e rastreamento das operações realizadas na base de dados com privilégios, em conformidade com o previsto no item 10.10.4 da NBR ISO/IEC 17799:2005;

9.2.28. implemente trilhas de auditoria para as atualizações no Índice Nacional do Infoseg, em conformidade com o previsto no item 10.10.1 da NBR ISO/IEC 17799:2005, contendo, no mínimo, a data-hora da alteração, o dado alterado e a identificação do responsável pela alteração;

9.2.29. implemente trilhas de auditoria para as concessões e revogações das contas de HOST do Infoseg, em conformidade com o previsto no item 10.10.1 da NBR ISO/IEC 17799:2005;

Acórdão 1832/2006 - Plenário

9.2.17 implante mecanismos nos sistemas da dívida, de modo que não haja possibilidade de alteração de informações e de decisões já processadas e que, em qualquer manuseio de informação ou qualquer tomada de decisão estratégica, que envolva altos volumes de recursos, ou outras decisões com nível de

importância similar, fique registrada a autoria, com a identificação do servidor, devendo os sistemas permitir que o controle possa rastrear qualquer operação realizada, de forma que estes mesmos sistemas não permitam que haja qualquer condição de burlar informações ex-post;

Acórdão 1663/2006 - Plenário

9.1.1. inclua nos arquivos log existentes no Sipiá, as informações relativas às alterações efetuadas;

Acórdão 2023/2005 - Plenário

9.4.10. altere o sistema de gerência de acessos para que nele sejam acrescentadas trilhas de auditoria para permitir futuras investigações de concessão e revogação de acesso de usuários aos sistemas [...], contendo, entre outras, informações sobre as datas e os responsáveis por essas concessões e revogações;

9.5.1. retire do sistema CPMR a possibilidade de exclusão física de processos; o processo pode ser excluído desde que todas as suas informações, inclusive as da exclusão, continuem registradas no sistema;

9.5.2. implemente rotinas que mantenham o registro de eventos relevantes do sistema CPMR; esses registros devem conter, no mínimo, o autor, a data e a descrição do evento;

Acórdão 782/2004 - 1ª Câmara

9.2.2. inclua, no âmbito do planeamento de segurança do sistema de pagamento de pessoal [...], a análise regular e sistemática dos registos (logs) de sistema operacional e do próprio sistema de pagamento;

9.2.3. utilize, preferencialmente, ferramentas de auditoria, como softwares especializados, na análise dos registos (logs) de sistema a serem efetuadas;

Acórdão 461/2004 - Plenário

9.1.4. a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;

Decisão 1380/2002 - Plenário

8.1.1.1 crie arquivo contendo histórico das operações realizadas;

Decisão 1098/2002 - Plenário

8.2.9 manutenção de logs de concessão de acesso e de autorização, permitindo consultas rápidas;

Decisão 1049/2000 – Plenário

8.3.13. adote providências com vistas a:

b) manter um histórico das alterações efetuadas nos bancos de dados, juntamente com suas justificativas, com vistas a fundamentar decisões tomadas, assim como dar subsídios a decisões futuras;

8.4.2. adote medidas visando agilizar a implementação dos produtos do Projeto DAP 12, atentando para procedimentos relativos ao programa de segurança, especialmente quanto a: análise dos logs e relatórios de violações dos procedimentos de segurança; proteção dos logs contra destruição intencional ou acidental; violações de segurança; e tentativas frustradas de acesso ao sistema;

Decisão 918/2000 - Plenário

8.2.6.9. adotar procedimentos de análise regular de arquivos tipo log, visando detectar eventuais violações ou tentativas de violação dos procedimentos de segurança;

8.2.9. implemente meios e procedimentos voltados à gerência de problemas relativos ao seu ambiente computacional, adotando, se possível, software adequado para essa finalidade, bem como análise sistemática das falhas verificadas, mantendo os respectivos registos históricos com o fito de promover ações preventivas nessa área;

Decisão 445/1998 - Plenário

3.7.18. realizar o controle diário, no SFG e FGI, das alterações efetuadas nos dados cadastrais de empregados, principalmente no que se refere aos dados que qualificam o titular da conta, nome de empregado, número do PIS/Pasep e número da Carteira de Trabalho e Previdência Social;

3.7.19. aprimorar os recursos hoje existentes nos sistemas SFG e FGI referentes a consultas de alterações efetuadas em dados cadastrais de empregados com vistas a melhor adequá-las ao controle, facilitando o acompanhamento das transações processadas;

3.7.20. elaborar procedimentos, consultas/relatórios, que possibilitem o controle concomitante das alterações processadas no Sistema de Controle de Empréstimos e Refinanciamentos - CER;

3.7.22. elaborar consultas on-line no Sistema de Controle de Segurança, SSG, e rever as já existentes no intuito de possibilitar um acompanhamento mais rigoroso por parte dos responsáveis pelo controle de acesso lógico aos sistemas;

4.16 De que trata a seção “Controle de acessos”?

Essa seção da norma orienta a direção quanto aos controles de acesso à informação e aos recursos de processamento das informações. São fornecidas diretrizes para definição de requisitos de negócio para controle de acesso, gerenciamento

de acesso e responsabilidades do usuário, controle de acesso à rede, sistema operacional, aplicação e informação, e, por fim, aspectos sobre computação móvel e trabalho remoto. Tais diretrizes englobam desde a definição de uma política de controle de acesso e o gerenciamento de privilégios até o isolamento de sistemas sensíveis.

4.17 Que acórdãos e decisões do TCU tratam, entre outros aspectos, do “Controle de acessos”?

Requisitos de negócio para controle de acesso

Acórdão 1092/2007 - Plenário

9.1.5. defina e divulgue Política de Controle de Acesso - PCA conforme o estabelecido na NBR ISO/IEC 17799:2005, item 11.1.1;

Acórdão 71/2007 - Plenário

9.2.7. defina formalmente uma Política de Controle de Acesso - PCA - para o Infoseg, contemplando usuários Web, “host de atualização” e da rede interna da gerência do Infoseg, de acordo com o previsto no item 11.1.1 da NBR ISO/IEC 17799:2005;

Acórdão 1663/2006 - Plenário

9.1.2. estabeleça processo formal de concessão de senhas e aumente o controle sobre os privilégios dos usuários;

Acórdão 2023/2005 - Plenário

9.1.3. defina uma Política de Controle de Acesso aos ativos de informação que contenha, no mínimo:

Decisão 295/2002 - Plenário

8.1.1 - quanto aos sistemas informatizados:

g) proceda à reavaliação completa dos perfis definidos no Senha-Rede para o SPIU, excluindo aqueles redundantes ou que não mais sejam utilizados;

Decisão 445/1998 – Plenário

3.7.4. criar controle único de acesso lógico para o ambiente do Gerenciador de Banco de Dados DB2, a exemplo do SSG no ambiente IDMS;

3.7.5. definir regras que regulamentem o acesso de usuários externos ao ambiente computacional do FGTS;

Gerenciamento de acesso do usuário

Acórdão 71/2007 - Plenário

9.2.8. conduza, a intervalos regulares, a análise crítica dos direitos de acesso dos usuários do Infoseg, por meio de um processo formal, de acordo com o previsto no item 11.2.4 da NBR ISO/IEC 17799:2005;

9.2.25. utilize identificadores de usuários únicos para o Infoseg (senha única não compartilhada) de forma fixar a responsabilidade de cada usuário, inclusive para os usuários com privilégios de administração, em conformidade com o previsto no item 11.2.1 da NBR ISO/IEC 17799:2005;

9.2.27. atribua a cada usuário do banco de dados do Infoseg somente os privilégios mínimos necessários ao desempenho de suas funções, conforme previsto no item 11.2.2 da NBR ISO/IEC 17799:2005;

Acórdão 1663/2006 - Plenário

9.1.2. estabeleça processo formal de concessão de senhas e aumente o controle sobre os privilégios dos usuários;

Acórdão 2023/2005 - Plenário

9.1.3.1. regras de concessão, de controle e de direitos de acesso para cada usuário e/ou grupo de usuários de recursos computacionais de Tecnologia da Informação - TI, conforme preceitua o item 9.1.1 da NBR ISO/IEC 17799:2001;

9.1.3.2. responsabilidades dos gestores de negócios sobre os seus sistemas, bem como a obrigação deles e dos gerentes da rede [...] fazerem a revisão periódica, com intervalos de tempo previamente definidos, dos direitos de acesso dos usuários, conforme prevêm os itens 9.2.1, incisos h e i, e 9.2.4 da NBR ISO/IEC 17799:2001;

9.1.3.3. obrigatoriedade de usuários de recursos de TI e gestores de negócios assinarem termos de compromisso nos quais estejam discriminados os direitos de acesso, os compromissos assumidos e suas responsabilidades e as sanções em caso de violação das políticas e dos procedimentos de segurança organizacional, a teor do que prescreve o item 9.2.1 da NBR ISO/IEC 17799:2001;

9.4.5. reveja a política de acesso do perfil administrador dos sistemas para que lhe sejam retirados:

9.4.5.1. o poder de criação de novos perfis e cadastro de usuários, centralizando essas funções e responsabilidades nos gestores de negócio;

9.4.5.2. o acesso irrestrito e permanente aos sistemas de produção;

Acórdão 782/2004 - 1ª Câmara

9.2.1. adote procedimentos formais de concessão e de validação periódica de senhas de usuários de sistemas informatizados, bem como de cancelamento de acesso de usuários que são desligados da unidade;

Acórdão 461/2004 - Plenário

9.1.3. a elaboração de lista de pessoas autorizadas a ter acesso aos servidores centrais, bem como, a sua revisão periódica;

9.1.6. a classificação do nível de segurança e controle de acesso aos dados, no âmbito do Projeto "Repositório";

Decisão 1098/2002 - Plenário

8.2.8 implementação da rotina de conformidade de operadores, nos moldes da existente no Sistema SIAFI, conforme já determinado por este Tribunal;

Decisão 295/2002 - Plenário

8.1.1 - quanto aos sistemas informatizados:

b) reveja as habilitações de todos os usuários do SIAPA lotados na [...], reavaliando não apenas sua permanência na Secretaria, como também seu local de trabalho (gerência) e a pertinência dos níveis de acesso concedidos;

c) proceda à reavaliação geral das pessoas habilitadas no SIAPA, particularmente com relação àquelas lotadas em outros órgãos/entidades, como o SERPRO;

e) estabeleça controle sistemático e oriente as Gerências Regionais da [...] quanto à necessidade de revisão dos níveis de acesso e acerto do local de trabalho, no Senha-Rede, quando da mudança de lotação de servidores da [...];

h) reveja as habilitações de todos os usuários do SPIU, lotados na [...] ou não, reavaliando sua

permanência no órgão e a pertinência dos níveis de acesso concedidos, assim como os inúmeros acessos concedidos a funcionários lotados no SERPRO, inclusive pertencentes à equipe de manutenção do sistema;

Decisão 1049/2000 - Plenário

8.1.8. adote medidas com vistas a manter o controle sobre as rotinas que fogem à regra geral de concessão ou atualização de benefícios, como a transação AEB – Atualização Especial de Benefício e aquelas com base em decisões judiciais (regidas pelos Despachos 03 e 04), de forma a impedir acesso indevido às transações on-line;

8.3.6. adote as seguintes medidas, quanto ao controle de acesso aos sistemas:

b) efetivação de estudos no sentido de obrigar a confirmação de acesso de usuários, por gestor, nos moldes, por exemplo, da Conformidade de Operadores do sistema SIAFI;

Decisão 918/2000 - Plenário

8.1.5. estude a viabilidade de instituir dispositivos de gerenciamento de acesso dos aplicativos do SIH/SUS (senhas, funções e relatórios de controle, logs etc.), quanto às funções de cadastramento, validação e envio das AIHs pelos gestores locais do SUS e das unidades prestadoras de serviços;

8.2.6.4. adotar procedimentos regulares para atualização das listas de acesso aos recursos computacionais;

8.2.6.5. observar com rigor os procedimentos formais para adicionar indivíduos à lista de pessoas autorizadas a ter acesso aos recursos computacionais, bem como adotar procedimentos específicos para a concessão de acessos emergenciais e/ou temporários;

8.2.6.7. implementar controles de segurança para as senhas de acesso, incluindo: exigência de alterações periódicas de senhas, evitando a sua repetição; estabelecimento de regras seguras para a definição de senhas pelos usuários, que exijam o número mínimo de caracteres definido nos padrões usuais para ambientes de informática (em regra, pelo menos seis caracteres); adoção de senhas iniciais distintas, fornecidas pela área de segurança lógica, para os usuários (abolindo o uso de senha inicial única); implementação de rotinas de suspensão de códigos de identificação de usuário ou de desabilitação de terminal ou microcomputador após um determinado número de tentativas de violação de segurança;

Responsabilidades dos usuários

Acórdão 914/2006 - Plenário

9.5.5. implemente as regras de formação de senhas, para vedar a utilização de senhas triviais, que fragilizem a segurança do sistema, utilizando, por exemplo, suas normas internas;

Acórdão 2023/2005 - Plenário

9.1.3.5. requisitos mínimos de qualidade de senhas, descritos pelo item 9.3.1 da NBR ISO/IEC 17799:2001;

9.1.7. informe seus usuários quanto à necessidade de bloquearem suas estações de trabalho quando delas se afastarem e de não compartilharem suas senhas de acesso, conforme prevê o item 9.3.2 da NBR ISO/IEC 17799:2001;

9.1.8. informe seus usuários quanto à necessidade de criarem senhas que satisfaçam aos requisitos mínimos definidos na Política de Controle de Acesso que vier a ser estabelecida e quanto à importância da qualidade e segurança das senhas;

Acórdão 782/2004 – 1ª Câmara

9.3.8. adote providências para que os papéis e documentos que contenham informações relevantes sobre o pagamento de pessoal sejam adequadamente guardados em armários ou gavetas, com fechaduras ou outras formas de proteção, especialmente fora do horário normal de serviço;

Decisão 918/2000 - Plenário

8.2.6.7. implementar controles de segurança para as senhas de acesso, incluindo: exigência

de alterações periódicas de senhas, evitando a sua repetição; estabelecimento de regras seguras para a definição de senhas pelos usuários, que exijam o número mínimo de caracteres definido nos padrões usuais para ambientes de informática (em regra, pelo menos seis caracteres); adoção de senhas iniciais distintas, fornecidas pela área de segurança lógica, para os usuários (abolindo o uso de senha inicial única); implementação de rotinas de suspensão de códigos de identificação de usuário ou de desabilitação de terminal ou microcomputador após um determinado número de tentativas de violação de segurança;

8.2.6.8. divulgar internamente a necessidade de preservação do sigilo das senhas;

Decisão 445/1998 - Plenário

3.7.29. disseminar que haja maior cuidado na criação e utilização de senhas entre usuários de sistemas do FGTS a fim de evitar fraudes;

Controle de acesso ao sistema operacional

Acórdão 71/2007 - Plenário

9.2.26. estabeleça procedimentos formais para a execução de operações diretamente sobre as bases de dados do Infoseg com a utilização de utilitários, documentando os procedimentos realizados, em conformidade com o previsto no item 11.5.4 da NBR ISO/IEC 17799:2005;

Acórdão 2023/2005 - Plenário

9.1.3.6. procedimentos de troca periódica de senhas, não permitindo reutilização das últimas, conforme prevê o item 9.5.4 da NBR ISO/IEC 17799:2001;

9.1.3.7. procedimentos de bloqueio de contas de usuários após longos períodos de não utilização ou de várias tentativas de acesso sem sucesso;

9.4.6. estude a possibilidade de implantação de procedimentos de segurança que bloqueiem as estações de trabalho e/ou sistemas após determinado período de não-utilização;

Acórdão 441/2005 - 1ª Câmara

1.1 inclua nas rotinas de acesso ao Sisfin, após a entrada no Sistema com sucesso, a apresentação das informações ao usuário da data e hora de última entrada válida no Sisfin;

1.9 realize estudos e implemente o melhor procedimento que proteja o set-up de seus computadores através do uso de senhas seguras, impedindo, especialmente, que os sistemas operacionais possam ser inicializados através de disquetes ou CDs;

Decisão 918/2000 - Plenário

8.2.6.7. [...] implementação de rotinas de suspensão de códigos de identificação de

usuário ou de desabilitação de terminal ou microcomputador após um determinado número de tentativas de violação de segurança;

Controle de acesso à aplicação e à informação

Acórdão 2023/2005 - Plenário

9.4.5. reveja a política de acesso do perfil administrador dos sistemas para que lhe sejam retirados:

9.4.5.1. o poder de criação de novos perfis e cadastro de usuários, centralizando essas funções e responsabilidades nos gestores de negócio;

9.4.5.2. o acesso irrestrito e permanente aos sistemas de produção;

Decisão 1380/2002 - Plenário

8.1.1.3 crie mecanismo de proteção quanto ao acesso aos dados do operador Super por intermédio do extrator de dados ou transação CONUSU;

4.18 De que trata a seção “Aquisição, desenvolvimento e manutenção de sistemas de informação”?

Essa seção da norma orienta a direção quanto à definição dos requisitos necessários de segurança

de sistemas de informação, medidas preventivas contra processamento incorreto das aplicações, uso de controles criptográficos, além de fornecer diretrizes para a segurança dos arquivos de sistema, segurança em processos de desenvolvimento e suporte, e gestão de vulnerabilidades técnicas.

4.19 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Aquisição, desenvolvimento e manutenção de sistemas de informação”?

Processamento correto nas aplicações

Acórdão 71/2007 - Plenário

9.2.3. institua mecanismos que garantam a consistência entre o Índice Nacional - IN - e as bases dos entes que alimentam o IN, verificando periodicamente a eficácia dos mecanismos implementados, de acordo com o previsto no item 12.2.2, da NBR ISO/IEC 17799:2005;

Decisão 595/2002 - Plenário

8.1.9 recomendar à Divisão de Modernização e Informática - Diminf que seja incluída uma validação na entrada de dados capaz de minimizar os erros de digitação dos pedidos de registros na base de dados de marcas, evitando assim a republicação do pedido;

Decisão 918/2000 - Plenário

8.1.2. estude [...] a viabilidade de implantar no SIH/SUS e no SIA/SUS maior número de críticas automáticas sobre quantitativos informados em AIHs, BPAs e APACs, baseadas em indicadores e padrões preestabelecidos a partir de médias históricas locais ou regionais, de modo a detectar eventuais distorções nas informações enviadas [...] pelos prestadores de serviço, visando melhorar o controle de fraudes nesses sistemas;

8.1.3. envide esforços para adequar o SIH/SUS e o SIA/SUS à realização de críticas automáticas com base na FCES, em substituição progressiva à FCH e à FCA, com vistas a melhorar a eficiência do controle de AIHs, BPAs e APACs, proporcionalmente ao grau de implementação da FCES no atendimento hospitalar e ambulatorial;

8.1.4. aprimore os módulos de CADASTRO do SIH/SUS e do SIA/SUS, com vistas a: minimizar as possibilidades de inserção de dados incorretos durante a digitação, bem como tornar mais auto-explicativas as respectivas telas do sistema, mediante a adição de teclas de atalho para tabelas (a exemplo das teclas “F1”, de ajuda ou help), acionáveis diretamente a partir dos campos de preenchimento e para textos explicativos;

8.1.6. envide esforços para automatizar o controle de qualidade do processamento do SIH/SUS (conferência da regularidade do processamento mensal), bem como o processo de disponibilização dos respectivos arquivos de saída na BBS/MS;

8.1.7. estude a viabilidade de implantar uma rotina de crítica automática no SIA/SUS, com o objetivo de conferir o volume de informações contidas em cada remessa mensal dos gestores locais do SUS com os volumes estatisticamente previstos, com base em padrões preestabelecidos;

Decisão 445/1998 - Plenário

3.7.9. revisar os procedimentos de crítica dos Sistemas de Controle de Contas Ativas e Inativas, SFG e FGI, a fim de que não permitam a inserção de contas vinculadas com PIS/PASEP viciados, de nomes com apenas uma palavra, com letras repetidas mais que duas vezes consecutivamente e com espaços em branco excedentes entre palavras;

3.7.10. revisar as rotinas de crítica do SFG/FGI quanto à inserção de contas vinculadas com PIS/PASEP inválido ou inexistente na base de dados;

3.7.11. sanear as bases de contas vinculadas ativas e inativas quanto à existência de contas com saldo negativo e não mais permitir sua ocorrência;

3.7.12. revisar as rotinas de crítica do SFG quanto à inserção de empresas com CGC inválido ou inexistente na base de dados;

3.7.13. inserir críticas no SFG com vistas a não permitir mais de um depósito na mesma conta vinculada para uma mesma competência;

3.7.14. revisar rotina de consulta do FGI, visto que algumas contas não são localizadas quando o argumento de pesquisa é o PIS/Pasep;

3.7.15. revisar rotina de pagamento quanto à exigência do PIS/Pasep correto;

3.7.16. revisar os procedimentos de crítica do CER quanto à inserção ou à alteração de dados cadastrais, como juros de mora, índice de reajuste, prazo de carência, dia de pagamento, dados de retorno;

Controles criptográficos

Acórdão 782/2004 - 1ª Câmara

9.3.9. estude [...] a possibilidade de utilizar recursos de criptografia e validação digital na proteção dos arquivos a serem gerados pelo programa FAP Digital em suas futuras versões;

Decisão 918/2000 - Plenário

8.2.4. adote providências para dificultar a alteração de dados nas tabelas do programa SIA.exe, incluindo, se necessário, os mesmos mecanismos de controle adotados no SIH/SUS (campos de controle criptografados);

8.2.6.6. abster-se de usar chaves públicas de acesso à rede, sem estarem associadas a um responsável;

Segurança em processos de desenvolvimento e de suporte

Acórdão 71/2007 - Plenário

9.2.12. estabeleça procedimentos formais de controle de demandas e de mudanças no Infoseg, de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas no item A16.2 do COBIT 4.0;

Acórdão 1663/2006 - Plenário

9.1.4. implemente sistemática de homologação e controle das versões implantadas do Sípia;

Acórdão 2023/2005 - Plenário

9.4.2. crie e defina mecanismos de gerenciamento que garantam a guarda e recuperação das versões atualizadas da documentação de sistemas pelo setor responsável;

9.4.4. adote cláusulas contratuais para assegurar que a documentação técnica, programas fontes e dados de sistemas regidos por contratos de prestação de serviços estejam acessíveis ao Ministério;

4.20 De que trata a seção “Gestão de incidentes de segurança da informação”?

Essa seção da norma orienta a direção para que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados e gerenciados de forma consistente e efetiva, permitindo a tomada de ação corretiva em tempo hábil. São fornecidas diretrizes para notificação de eventos e fragilidades de segurança da informação, definição de responsabilidades e procedimentos de gestão desses eventos e fragilidades, além da coleta de evidências e do estabelecimento de mecanismos para análise dos incidentes recorrentes ou de alto impacto com vistas à sua quantificação e monitoramento.

4.21 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Gestão de incidentes de segurança da informação”?

Acórdão 71/2007 - Plenário

9.1.3. implemente serviço de atendimento ao usuário do Infoseg (help desk) adequado às suas necessidades, em conformidade com o previsto no item 13.1.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas no DS8.1 do COBIT 4.0, avaliando a conveniência de implantá-lo em regime ininterrupto (24 horas por dia e 7 dias por semana);

Acórdão 782/2004 – 1ª Câmara

9.2.4. e 9.3.4. adote um programa de treinamento específico para a área de segurança de sistemas, enfocando aspectos de segurança física e lógica, bem assim a reação dos funcionários frente à ocorrência de contingências que possam afetar a continuidade dos serviços;

4.22 De que trata a seção “Gestão da continuidade do negócio”?

Essa seção da norma orienta a direção quanto às medidas a serem tomadas para prevenir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos, falhas ou desastres significativos, assegurando sua retomada em tempo hábil, se for o caso. São fornecidas diretrizes para incluir a segurança da informação no processo de gestão da continuidade de negócio e para realizar análise e avaliação de riscos, além de desenvolver, implementar, testar e reavaliar planos de continuidade relativos à segurança da informação.

4.23 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Gestão da continuidade do negócio”?

Acórdão 1092/2007 - Plenário

9.1.6. implante a gestão de continuidade do negócio conforme o estabelecido na NBR ISO/

IEC 17799:2005, itens 14.1.1, 14.1.2 e 14.1.3, e elabore o Plano de Continuidade do Negócio - PCN conforme o estabelecido na NBR ISO/IEC 17799:2005, itens 14.1.4 e 14.1.5;

Acórdão 71/2007 - Plenário

9.2.14. defina formalmente um Plano de Continuidade do Negócio - PCN - específico para o Infoseg, que garanta em caso de falhas ou desastre natural significativo, a retomada em tempo hábil das atividades do sistema, protegendo os processos críticos, de acordo com o previsto nos itens 14.1.4 e 14.1.5 da NBR ISO/IEC 17799:2005;

Acórdão 1832/2006 - Plenário

9.1.3 implante um Plano de Contingência [...], com prioridade e atenção especial às áreas com grande exposição a riscos, às áreas envolvidas com elevados volumes de recursos e quantidade de transações, bem assim àquelas que possam trazer riscos de imagem à Instituição, observando-se as peculiaridades e características intrínsecas do [...];

Acórdão 2083/2005 - 2ª Câmara

9.3.7.1. crie normativos para a condução dos diversos serviços passíveis de acidentes, com manuais de procedimentos; ações mais efetivas da CIPA; promoção de encontros, seminários e palestras sobre o tema; propagandas visuais de conscientização e realização da SIPAT;

9.3.7.3. priorize as ações de prevenção, realizando cursos específicos, reciclagem e especializações;

Acórdão 461/2004 - Plenário

9.1.5. a elaboração e implementação de um Plano de Contingências de acordo com o item 11.1.4 da NBR ISO/IEC 17799:2001;

Decisão 1380/2002 - Plenário

8.3.3 elabore Plano de Contingências [...] que possa orientar os técnicos em caso de ocorrência de sinistros ou de situações que venham a comprometer a operação do sistema;

Decisão 1049/2000 - Plenário

8.3.4. adote as medidas recomendadas por sua Auditoria Interna [...] como por exemplo a implementação de um plano formal que contenha medidas de contingência e recuperação de processos;

Decisão 918/2000 - Plenário

8.2.6.1. elaborar plano de contingência, incluindo a previsão de testes de validação e de roteiros específicos para os procedimentos de contingência;

Decisão 445/1998 - Plenário

3.7.6. providenciar, com a maior brevidade possível, o Plano de Contingências;

Decisão 669/1995 - Plenário

2.1. estude a possibilidade de implementar, a médio prazo, no âmbito do seu plano de contingência, uma solução alternativa para o caso de perda total das instalações da Filial São Paulo, nas quais se opera o processamento da Arrecadação Federal, para que o tratamento das informações essenciais não sofra solução de continuidade no caso de ocorrência de sinistro de grande proporções;

4.24 De que trata a seção “Conformidade”?

Essa seção da norma orienta a direção a evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, além de garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação. São fornecidas diretrizes para identificação da legislação vigente, proteção dos direitos de propriedade intelectual, proteção dos registros organizacionais, proteção de dados e privacidade de informações pessoais, prevenção

de mau uso de recursos de processamento da informação e regulamentação de controles de criptografia. Além disso, são feitas algumas considerações quanto à auditoria de sistemas de informação.

4.25 Que acórdãos e decisões do TCU tratam, entre outros aspectos, da “Conformidade”?

Conformidade com requisitos legais

Acórdão 1832/2006 - Plenário

9.2.12 - adote procedimento especial para o registro e a tramitação de todos os documentos, que contenham, de algum modo, informações estratégicas e/ou privilegiadas;

Acórdão 2083/2005 - 2ª Câmara

9.3.11. abstenha-se da utilização de softwares não licenciados;

Conformidade com normas e políticas de segurança da informação e conformidade técnica

Acórdão 2023/2005 - Plenário

9.4.1. implemente os procedimentos informatizados necessários no sentido de ajudar

a garantir a observância das políticas e normas que venham a ser instituídas pelo Ministério, como a Política de Segurança da Informação, a Política de Controle de Acesso e a Metodologia para Desenvolvimento de Sistemas;

Decisão 445/1998 - Plenário

3.7.21. incorporar ao Sistema de Controle de Segurança, SSG, as restrições impostas pela norma de controle de acesso lógico, MN FG.01.05.00;

3.7.23. desautorizar prestadores de serviços que estejam habilitados de forma contrária à norma constante no MN FG.01.05.00;

Considerações quanto à auditoria de sistemas de informações

Acórdão 1092/2007 - Plenário

9.1.8. implante, por meio de sua Auditoria Interna, política de auditoria nos diversos sistemas de tecnologia da informação pertinentes à arrecadação de receitas da Empresa;

Referências bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**:2005: tecnologia da informação, técnicas de segurança, código de prática para a gestão da segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2005.

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 24 out. 2007.

_____. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acesso em: 24 out. 2007.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.



TRIBUNAL DE CONTAS DA UNIÃO

SAFS Quadra 4 lote 1

70042-900 Brasília-DF

<<http://www.tcu.gov.br>>

Responsabilidade Editorial

Secretário-Geral de Controle Externo
Jorge Pereira de Macedo

Secretário de Fiscalização de Tecnologia da Informação
Cláudio Souza Castello Branco

Elaboração
Cláudia Augusto Dias
Roberta Ribeiro de Queiroz Martins

Capa e Editoração

Secretaria-Geral da Presidência
Instituto Serzedello Corrêa
Centro de Documentação
Editora do TCU

Revisão de Texto

Focalize Eventos e Serviços Ltda.

Endereço para contato e solicitação de exemplares

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo II, Sala 311
70042-900 – Brasília-DF
Fone: (61) 3316.5371/7396
Fax: (61) 3316.5372
sefti@tcu.gov.br
<http://www.tcu.gov.br/fiscalizacaoti>

Impresso pela Sesap/Segedam

Secretaria de Fiscalização de Tecnologia da Informação

Negócio

Controle externo da governança de tecnologia da informação na Administração Pública Federal.

Missão

Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Visão

Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.

www.tcu.gov.br