TRIBUNAL DE CONTAS DA UNIÃO

Boas Práticas em Segurança da Informação

4ª edição

República Federativa do Brasil
Tribunal de Contas da União

Ministros

Benjamin Zymler
Presidente

Augusto Nardes
Vice-presidente

Valmir Campelo
Walton Alencar Rodrigues
Aroldo Cedraz
Raimundo Carreiro
José Jorge
José Múcio Monteiro
Ana Arraes

Ministros-substitutos

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

Ministério Público junto ao TCU

Lucas Rocha Furtado
Procurador-geral

Paulo Soares Bugarin
Subprocurador-geral

Cristina Machado da Costa e Silva
Subprocuradora-geral

Marinus Eduardo de Vries Marsico,
Júlio Marcelo de Oliveira,
Sérgio Ricardo Costa Caribé
procuradores

TRIBUNAL DE CONTAS DA UNIÃO

Boas Práticas em Segurança da Informação

4ª edição

Brasília, 2012

Brasil. Tribunal de Contas da União.

Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

103 p.

1. Segurança da informação 2. Tecnologia da informação. 3. Controle de acesso. 4. Segurança de dados. I. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

Apresentação

A Tecnologia da Informação (TI) exerce papel cada vez mais relevante para o as instituições da Administração Pública Federal (APF). Por isso, tem crescido também a importância de se proteger as informações e os ativos de TI com relação aos riscos e às ameaças que se apresentam nesta área.

Por estas razões, a segurança da informação tornou-se um ponto crucial à manutenção e ao avanço das instituições.

O Tribunal de Contas da União, ciente da relevância deste assunto, bem como da importância do papel pedagógico, elaborou esta publicação com intuito de despertar a atenção para os aspectos da segurança da informação nas instituições governamentais.

Espera-se que esse trabalho possa ajudar o Estado brasileiro a aprimorar a segurança da informação das instituições, contribuindo para que a tecnologia da informação agregue ainda mais valor ao negócio da Administração Pública Federal, em benefício da sociedade.

Ministro Benjamim Zmyler
Presidente

Sumário

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 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 métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das instituições 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 TI envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e os negócios da instituição, em especial, os gestores da Administração Pública Federal.

Esta quarta edição traz a mudança de nomenclatura com relação à norma ABNT NBR ISO/IEC 17799:2005, substituída pela norma ABNT NBR ISO/IEC 27002:2005, e acrescenta, no Capítulo 4, novas deliberações do Tribunal sobre segurança da informação. Ademais, nos três primeiros capítulos, foram feitas menções às normas de segurança da informação e comunicações do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Secretaria de Fiscalização de
Tecnologiada da Informação

1 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.

1.1 O que visa a segurança de informações?

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

1.1.1 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.

1.1.2 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.

1.1.3 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.

1.1.4 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 é de direito.

1.2 Por que é importante zelar pela segurança de informações?

Porque a informação é um ativo muito importante para qualquer instituição, 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 instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

1.3 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 instituição para que sejam assegurados seus recursos computacionais e suas informações.

1.4 Quem são os responsáveis por elaborar a PSI?

É recomendável que na estrutura da instituição 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 instituição 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 instituição.

1.5 Que assuntos devem ser abordados na PSI?

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

O conteúdo da PSI varia, de instituição para instituição, 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 instituição;
- 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.

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

A política de segurança de informações deve conter princípios, diretrizes e regras genéricos e amplos, para aplicação em toda a instituição. 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 instituição achar conveniente e necessário que a 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.

1.7 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 a não observância. Normalmente, após a consecução das três primeiras etapas, as gerências de segurança acreditam terem cumprido o dever e esquecem-se 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 alta administração;
- aprovação;
- publicação;
- divulgação;
- treinamento;
- implementação;
- avaliação e identificação das mudanças necessárias;
- revisão.

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

O sucesso da PSI está diretamente relacionado ao envolvimento e à atuação da alta administração. Quanto maior for o comprometimento da administração 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.

1.9 A quem deve ser divulgada a PSI?

A divulgação ampla a todos os usuários internos e externos à instituição 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 instituição e que, direta ou indiretamente, serão afetados por ela. É necessário que fique bastante claro, para todos, as consequências 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.

1.10 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 a severidade, a amplitude e o 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 instituição, 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 as causas, consequências 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.

1.11 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 a reavaliação a qualquer mudança que venha afetar a análise de risco original, tais como: incidente de segurança significativo, novas vulnerabilidades, mudanças organizacionais ou na infraestrutura 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.

1.12 Existem normas sobre PSI para a Administração Pública Federal?

O Decreto n.º 3.505, de 13.06.2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Em linhas gerais, os objetivos traçados nessa PSI dizem respeito à necessidade de capacitação e conscientização das pessoas lotadas nos órgãos e entidades da Administração Pública Federal quanto aos aspectos de segurança da informação; e necessidade de elaboração e edição de instrumentos jurídicos, normativos e organizacionais que 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 interoperabilidade, obtenção dos níveis de segurança desejados e permanente disponibilização dos dados de interesse para a defesa nacional;

O TCU, por meio do Acórdão 2471/2008 - Plenário, fez as seguintes recomendações ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

> 9.6.1. crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa;
>
> 9.6.2. identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal;

O GSI/PR editou, em 30/06/2009, a Norma Complementar 03/IN01/DSIC/GSIPR, que estabeleceu diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

2 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.

2.1 O que são controles de acesso?

Os controles de acesso, físicos ou lógico, 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.

2.2 O que são controles de acesso lógico?

Os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas de computador.

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

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

2.3 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 as 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 *log*s 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.

2.4 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.

2.5 Como os usuários são identificados e autenticados?

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

Normalmente esse processo envolve a entrada de um ID (identificação do usuário) e uma senha (autenticação do usuário). A identificação define para o computador quem é o usuário e a senha é um autenticador, isto é, ela prova ao computador que o usuário é realmente quem ele diz ser.

2.5.1 *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.

2.5.2 *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 por meio dos *log*s.

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.

2.5.3 *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*, *softwares* e procedimentos que permitem o acesso de usuários aos recursos computacionais.

Na autenticação, o usuário deve apresentar algo que só ele saiba ou possua, podendo até envolver a verificação de características físicas pessoais. A maioria dos sistemas atuais solicita uma senha (algo que, supostamente, só o usuário conhece), mas já existem sistemas mais modernos utilizando cartões inteligentes (algo que o usuário possui) ou ainda características físicas

(algo intrínseco ao usuário), como o formato da mão, da retina ou do rosto, impressão digital e reconhecimento de voz.

2.5.4 *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 instituição 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 tenha acesso.

2.5.5 *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 os caracteres estejam embaralhados;
- nome de membros de sua família ou de amigos íntimos;
- nomes de pessoas ou lugares em geral;
- nome do sistema operacional ou da máquina que está sendo utilizada;
- nomes próprios;
- datas;
- números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- placas ou marcas de carro;

- palavras que constam de dicionários em qualquer idioma;
- letras ou números repetidos;
- letras seguidas do teclado do computador (ASDFG, YUIOP);
- objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela);
- qualquer senha com menos de 6 caracteres.

Alguns *softwares* são capazes de identificar senhas frágeis, como algumas dessas citadas acima, a partir de bases de dados de nomes e sequências 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.

2.5.6 *Como escolher uma boa senha?*

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

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

2.5.7 *Como deve ser feita a concessão de senhas aos usuários?*

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

- solicitar aos usuários a assinatura de uma declaração, a fim de manter

a confidencialidade de sua senha pessoal (isso pode estar incluso nos termos e condições do contrato de trabalho do usuário);
- garantir, aos usuários, que estão sendo fornecidas senhas iniciais seguras e temporárias, forçando-os a alterá-las logo no primeiro *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 mensagens de correio eletrônico desprotegidas (não criptografadas) deve ser evitado.

2.5.8 *O que a instituição pode fazer para proteger e controlar as senhas de acesso aos 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 frequente 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 frequente 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, a segurança.

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

Ex-funcionários devem ter suas senhas bloqueadas. Para isso, devem existir procedimentos administrativos eficientes que informem o gerente de segurança, ou o administrador dos sistemas, da ocorrência de demissões ou desligamentos de funcionários. Esses procedimentos, na prática, nem sempre são seguidos, expondo a instituição a riscos indesejáveis.

Também devem ser bloqueadas contas de usuários após um determinado número de tenta-

tivas 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.

2.5.9 *Existem outras formas de autenticação do usuário, além do uso de senhas?*

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

2.5.10 *O que são* tokens*?*

A ideia de fornecer *tokens* aos usuários como forma de identificá-los é bastante antiga. No nosso dia-a-dia estamos frequentemente utilizando *tokens* para acessar alguma coisa. A chave que abre a porta da residência ou o 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 conta bancária.

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

2.5.11 *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 a utilização por outras pessoas que não os proprietários legítimos.

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

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

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

2.5.12 *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.

2.5.13 *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 a alta taxa de erro, em função da mudança das características de uma pessoa com o passar dos anos, ou devido a problemas de saúde ou nervosismo, por exemplo. A tolerância a erros deve ser estabelecida com precisão, de forma a não ser grande o suficiente para admitir impostores, nem pequena demais a ponto de negar acesso a usuários legítimos. Abaixo serão apresentadas algumas características humanas verificadas por sistemas biométricos existentes:

- impressões digitais – são características únicas e consistentes. Nos sistemas biométricos que utilizam essa opção, são armazenados de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão lida com impressões digitais de pessoas autorizadas, armazenadas em sua base de dados. Atualmente, estão sendo utilizadas impressões digitais em alguns sistemas governamentais, como por exemplo, o sistema de previdência social na Espanha e o de registro de eleitores na Costa Rica;
- voz – os sistemas de reconhecimento de voz são usados para controle de acesso, porém não são tão confiáveis quanto às impressões digitais, em função dos erros causados por ruídos do ambiente e problemas de garganta ou nas cordas vocais das pessoas a eles submetidas;
- geometria da mão – também é usada em sistemas de controle de acesso, porém essa característica pode ser alterada por aumento ou diminuição de peso ou artrite;

- configuração da íris e da retina – os sistemas que utilizam essas características se propõem a efetuar identificação mais confiável do que os sistemas que verificam impressões digitais. Entretanto, são sistemas invasivos, pois direcionam feixes de luz aos olhos das pessoas que se submetem à sua identificação;
- reconhecimento facial por meio de termogramas - o termograma facial é uma imagem captada por uma câmera infravermelha que mostra os padrões térmicos de uma face. Essa imagem é única e, combinada com algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se em uma técnica não invasiva, altamente confiável, não sendo afetada por alterações de saúde, idade ou temperatura do corpo. São armazenados ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. O desenvolvimento dessa tecnologia tem como um de seus objetivos baratear seu custo para que possa ser usada em um número maior de aplicações de identificação e autenticação.

2.6 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 instituição. Esse controle pode ser feito por menus, funções ou arquivos.

2.6.1 *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 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.

2.6.2 *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 restrição de acesso a funções de acordo com o usuário (menus de acesso predefinidos), horário ou tipo de recursos (impressoras, fitas *backup*).

2.6.3 *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.
- 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, neste caso, é a matriz de controle de acesso. Nesta matriz, pode-se fazer duas análises: uma em relação aos sujeitos; outra, em relação aos objetos.

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

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

2.6.5 *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.

2.7 Como monitorar o acesso aos recursos informacionais?

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

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

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

2.7.1 *O que são* logs*?*

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

Os *logs* são utilizados como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de *logon* ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando. Com os dados dos *logs*, pode-se identificar e corrigir falhas da estratégia de segurança. Por conterem informações essenciais à 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.

2.7.2 *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.

2.8 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 simultanea-

mente. 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.

2.9 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.

2.9.1 *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.

2.9.2 *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.

2.9.3 *Que tipo de regras de controle de acesso devem ser formalizadas na política?*

O acesso aos sistemas de informação deve ser controlado mediante 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 instituição;
- fornecimento, aos usuários, de documento escrito com seus direitos de acesso. Os usuários deverão assinar esse documento, indicando que entenderam as condições dos 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 instituição;
- 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.

2.10 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.

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

A cooperação dos usuários autorizados é essencial à 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.

2.12 Existem normas sobre controles de acesso lógico para a Administração Pública Federal?

O TCU, por meio do Acórdão 2471/2008 - Plenário, fez as seguintes recomendações ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

> 9.6.1. crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa;
> 9.6.2. identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal;

O GSI/PR editou, em 06/05/2010, a Norma Complementar 07/IN01/DSIC/GSIPR, que estabeleceu diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3 Plano de Continuidade do Negócio

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

3.1 O que é Plano de Continuidade do Negócio - PCN?

Plano de Continuidade do Negócio 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 Continuidade do Negócio é um conjunto de medidas que combinam ações preventivas e de recuperação.

Obviamente, os tipos de riscos a que estão sujeitas as instituições variam no tempo e no espaço. No entanto, 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 Continuidade do Negócio pode ser desenvolvido por instituições que contenham ou não sistemas computadorizados. Porém, para efeito desta cartilha, o Plano se aplica às instituições que, em menor ou maior grau, dependem da tecnologia da informação, pois se faz 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 PCN?

Atualmente, é inquestionável a dependência das instituições aos computadores, sejam eles de pequeno, médio ou grande porte. Esta característica quase generalizada, por si só, já é capaz de explicar a importância do Plano de Continuidade do Negócio, pois, se para fins de manutenção dos serviços, as instituições dependem de

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

Por conseguinte, pode-se considerar o Plano de Continuidade do Negócio quesito essencial para as instituições preocupadas com a segurança de suas informações.

3.3 Qual é o objetivo do PCN?

O objetivo do Plano de Continuidade do Negócio é manter a integridade e a disponibilidade dos dados da instituição, bem como a disponibilidade dos 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 PCN?

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

- riscos a que está exposta a instituição, probabilidade de ocorrência e os impactos decorrentes (tanto aqueles relativos à escala do dano como ao tempo de recuperação);
- consequências 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 PCN?

De maneira geral, o Plano de Continuidade do Negócio 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 instituição. Quanto mais o aplicativo influenciar na capacidade de funcionamento da instituição, 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;
- instituições 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 administração na elaboração do PCN?

É imprescindível o comprometimento da alta administração com o Plano de Continuidade

do Negócio. Na verdade, este Plano é de responsabilidade direta da alta administração, é um problema corporativo, pois trata de estabelecimento de procedimentos que garantirão a sobrevivência da instituição como um todo e não apenas da área de informática. Ainda, muitas das definições a serem especificadas são definições relativas ao negócio da instituição e não à tecnologia da informação.

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

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

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

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

3.7 Como garantir que o Plano funcionará como esperado?

É possível citar três formas de garantir a eficácia do Plano de Continuidade do Negócio: 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 Continuidade do Negócio.

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 PCN 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 Continuidade do Negócio deverá ser testado. Ele pode ser testado na 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 PCN?*

Mudanças que tenham ocorrido e que não estejam contempladas no Plano de Continuidade do Negócio 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 clienteschave;
- de processos (inclusões e exclusões);
- no risco (operacional e financeiro).

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

3.8 Existem normas sobre PCN para a Administração Pública Federal?

O TCU, por meio do Acórdão 2471/2008 - Plenário, fez as seguintes recomendações ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

> 9.6.1. crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa;
> 9.6.2. identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal;

O GSI/PR editou, em 11/11/2009, a Norma Complementar 06/IN01/DSIC/GSIPR, que estabeleceu diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 TCU e a NBR ISO/IEC 27002:2005

Neste capítulo será comentada a NBR ISO/IEC 27002:2005 como norma técnica de auditoria de segurança da informação utilizada pelo 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 do Tribunal que tratam, entre outros aspectos, de segurança da informação. Registra-se que a listagem de acórdãos do Tribunal referente a cada seção da norma não é exaustiva.

4.1 De que trata a NBR ISO/IEC 27002:2005?

A NBR ISO/IEC 27002:2005, 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 internacional ISO/IEC 27002:2005.

Destaca-se que essa norma é a sucessora da ABNT NBR ISO/IEC 17799:2005 (utilizada nas edições anteriores desta cartilha), sendo que essa nova edição visou basicamente à adequação à nova nomenclatura da ISO (*International Organization for Standardization*), não havendo alteração quanto ao conteúdo em si da NBR ISO/IEC 17799:2005. Portanto, não se trata propriamente de uma nova versão.

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 e IEC (*International Eletrotechnical Commission*), autoras da norma, são mundialmente reconhecidas pela capacitação técnica. A norma ISO/IEC 27002:2005, 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 provem 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 27002:2005 configura-se como um dos melhores critérios de auditoria de segurança da informação disponível até a data de publicação desta cartilha. Nos acórdãos e decisões, o Tribunal já mencionou a versão de 2005 dessa norma (NBR ISO/IEC 27002 e NBR ISO/IEC 17799) e a versão de 2001.

4.3 Como o TCU avalia a segurança da informação na Administração Pública Federal?

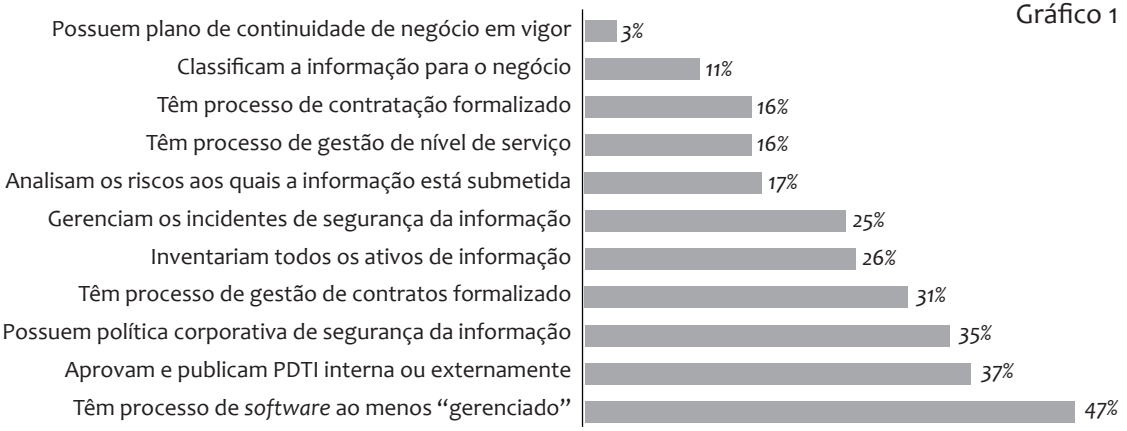
Em 2007, o TCU realizou o primeiro Levantamento de Governança de TI, que teve como um dos objetivos "delinear a qualidade do tratamento dado pelos órgãos públicos à segurança das informações sob sua responsabilidade". Naquela oportunidade, a versão 17799:2005 da norma foi utilizada como critério de avaliação da governança de TI no que se refere aos aspectos de segurança da informação. Este Levantamento foi baseado num questionário de 39 perguntas respondido por 255 órgãos/entidades da administração pública federal.

Considerando que as constatações desse trabalho indicaram que a situação da gestão da segurança da informação era preocupante na maior parte dos órgãos/entidades pesquisados, o TCU, por meio do Acórdão 1.603/2008 - Plenário, recomendou ao Conselho Nacional de Justiça (CNJ), ao Conselho Nacional do Ministério Público (CNMP), à Diretoria-Geral do Senado Federal, à Diretoria-Geral da Câmara dos Deputados, ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e também à Secretaria-Geral da Presidência (Segepres) e à Secretaria-Geral de Administração (Segedam) do próprio Tribunal que:

> [...] orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

Em 2010, o TCU realizou novo Levantamento de Governança de TI, em que se utilizou a NBR ISO/IEC 27002:2005 como critério para avaliação da segurança da informação das instituições pesquisadas. O Levantamento foi baseado num questionário mais abrangente composto de 30 perguntas e 152 itens e foi respondido por 301 órgãos/entidades da administração pública federal. O Acórdão 2.308/2010-TCU-Plenário, decorrente deste trabalho, constatou a seguinte situação (demonstrada no gráfico da página a seguir) com relação à segurança da informação:

Gráfico 1



Seguem trechos do relatório do Acórdão 2.308/2010-TCU-Plenário.

> 75. Não se percebe melhora nos indicadores de segurança da informação em relação ao levantamento anterior, a despeito da recomendação emitida pelo TCU. A Administração, de forma geral, continua a desconhecer e a não proteger suas informações críticas adequadamente. Como não há avaliação de riscos, nem ao menos é possível estimar as suas consequências caso estes se materializem.
>
> 198. Na comparação com o levantamento de 2007, é preocupante a falta de evolução perceptível na área de segurança da informação, que continua com índices de não conformidade muito altos (seção 2.3) ...

Seguem trechos do voto do Relator, Ministro Aroldo Cedraz:

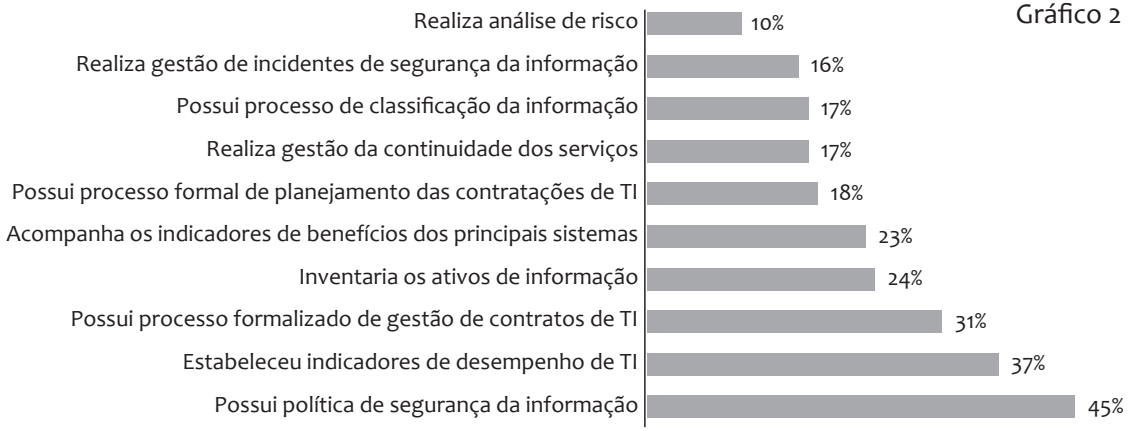
> 12. No que tange aos aspectos que já haviam sido examinados em 2007, as principais constatações do presente levantamento foram de que:
>
> c) nenhum dos indicadores relativos à segurança da informação, que envolve confidencialidade, integridade e disponibilidade da informação, apresentou avanço substancial, o que significa que, um ano e meio depois dos alertas formulados pelo acórdão 1.603/2008 - Plenário, a administração pública permanece exposta aos mesmos riscos, não tem agido para reduzi-los, não

consegue estimar suas consequências e continuar a desconhecer a não proteger suas informações críticas adequadamente.

20. Destaco, em especial, a imprescindibilidade de cumprimento dos comandos relativos ao aprimoramento da segurança da informação, aspecto que considero crucial para funcionamento de todas as organizações públicas, ante os riscos à integridade, confidencialidade e disponibilidade de dados e em face da ausência de qualquer evolução significativa nesse particular desde 2007.

Atendendo ao item 9.4.3 do Acórdão 2.308/2010-TCU-Plenário, o TCU voltou a realizar Levantamento de Governança de TI em 2012, como parte do processo de trabalho estabelecido pela Secretaria de Fiscalização de Tecnologia da Informação (Sefti), o qual prevê a realização de levantamento para acompanhar a situação de governança de TI a cada dois anos. A NBR ISO/IEC 27002:2005, entre outras, foi utilizada novamente como referência para avaliação da segurança da informação das instituições pesquisadas. O Levantamento foi baseado em questionário composto de 36 questões subdivididas em 494 itens e foi respondido por 337 órgãos/entidades da administração pública federal. O Acórdão 2.585/2012-TCU-Plenário, decorrente deste trabalho, constatou a seguinte situação com relação à segurança da informação:

Gráfico 2



Além da realização desses três levantamentos, o TCU, no âmbito de fiscalizações que analisaram a gestão e o uso da TI na APF, constatou várias fragilidades relacionadas ao tema segurança da informação. O resultado consolidador dessas fiscalizações foi proferido no Acórdão 1.233/2012-TCU-Plenário, que assim deliberou sobre o tema:

> 9.8. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que:
> 9.8.1. em atenção à Lei 10.683/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente à Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição);
> 9.8.2. em atenção a Lei 10.683/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II;
> 9.8.3. reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1.

4.4 Como está estruturada a NBR ISO/IEC 27002:2005?

A NBR ISO/IEC 27002, 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.

4.5 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 instituição. São fornecidas diretrizes para elaboração e análise crítica do documento.

4.5.1 Que acórdãos do TCU tratam, entre outros aspectos, de "Política de segurança da informação"?

(Textos extraídos de itens do Acórdão)

Acórdão 1233/2012 Plenário

9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8):

9.15.12.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

—

Acórdão 758/2011 Plenário

9.2.6. – em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VII, implante Política de Segurança da Informação e Comunicações, com observância das práticas da Norma Complementar 03/IN01/DSIC/GSIPR;

—

Acórdão 594/2011 Plenário

9.4.3. em atenção à IN GSI/PR 1/2008, art. 5º, VII, atualize a Política de Segurança da Informação e Comunicações;

(Textos extraídos de itens do Acórdão)

Acórdão 381/2011 Plenário	9.1.1. (...) promova o alinhamento da sua Política de Segurança da Informação e Comunicações às diretrizes nacionais, como a Norma Técnica – Gabinete de Segurança Institucional – Presidência da República – Norma Complementar 03/IN01/DSIC/GSIPR, também observando as práticas contidas na Norma Técnica – NBR – ISO/IEC 27002, item 5.1 – Política de segurança da informação, de sorte a contemplar também itens ainda não normatizados, tais como: diretrizes gerais sobre tratamento da informação, penalidades e Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), conforme tratado no Achado nº 12 – Falhas na Política de Segurança da Informação e Comunicações (POSIC), do Relatório de Fiscalização;
	—
Acórdão 2746/2010 Plenário	9.1.7. implante Política de Segurança da Informação e Comunicações, com observância da Norma Complementar 03/IN01/DSIC/GSIPR, em atenção à IN GSI/PR 01/2008, art. 5º, VII;
	—
Acórdão 1382/2009 Plenário	9.2. (...) defina e implante uma Política de Segurança da Informação para toda a organização, que estabeleça normas e princípios norteadores da gestão da segurança da informação no Ministério, alinhados aos objetivos de negócio do órgão, conforme orientações contidas na NBR ISO/IEC 17799:2005, item 5.1.1 - Documento da política de segurança da informação, e em à semelhança das orientações dispostas no Cobit 4.1, item DS5.2 - Plano de segurança de TI;

(Textos extraídos de itens do Acórdão)

Acórdão 906/2009 Plenário	9.1.1. elabore e formalize política de segurança da informação adequada às necessidades do órgão, que estabeleça os princípios norteadores da gestão de segurança da informação, em consonância com a Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008 [...] e à semelhança dos itens 5.1 da NBR ISO/IEC 27002:2005 e PO6.1 do Cobit 4.1;
	—
Acórdão 669/2008 Plenário	9.4.5. defina e implante uma Política de Segurança da Informação para toda a organização, que estabeleça normas e princípios norteadores da gestão da segurança da informação no Ministério, alinhados aos objetivos de negócio do órgão, conforme orientações contidas na NBR ISO/IEC 17799:2005, item 5.1.1, e em consonância com as orientações dispostas no item DS5.2 do Cobit 4.1 (Plano de segurança de TI);
	—
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;

(Textos extraídos de itens do Acórdão)

Acórdão 71/2007 Plenário	9.2.6. defina formalmente uma Política de Segurança da Informação - PSI - para o [Sistema], 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 [Sistema], de acordo com o previsto no item 5.1.1 da NBR ISO/IEC 17799:2005;
	—
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;

(Textos extraídos de itens do Acórdão)

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;

4.6 De que trata a seção "Organizando a segurança da informação"?

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

São fornecidas diretrizes para organizar a segurança da informação, detalhando aspectos da organização interna: comprometimento da direção, coordenação, atribuição de responsabilidades, processo de autorização para recursos de processamento da informação, acordos de confidencialidade, análise crítica independente, contato com autoridades e com 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.

4.6.1 *Que acórdãos do TCU tratam, entre outros aspectos, da "Organização da segurança da informação"?*

ORGANIZAÇÃO INTERNA
(Textos extraídos de itens do Acórdão)

Acórdão 1233/2012 Plenário	9.15.12 estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8): 9.15.12.1 nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação; 9.15.12.2 criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;
	—
Acórdão 866/2011 Plenário	9.2.4 em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VI, c/c Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.3, institua Comitê de Segurança da Informação e Comunicações, observando a NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação; 9.2.5 em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, IV, e art. 7º, c/c Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.2, nomeie Gestor de Segurança da Informação e Comunicações, observando a NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

Organização interna
(Textos extraídos de itens do Acórdão)

Acórdão 594/2011 Plenário

9.1.2 em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, IV, e art. 7º, c/c a Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.2, nomeie servidor para a função de Gestor de Segurança da Informação e Comunicações, observando as práticas contidas na NBR ISO/IEC 27002:2005, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

9.4.6 em atenção à IN GSI/PR 1/2008, art. 5º, VI, e art. 6º, assegure o funcionamento do Comitê de Segurança da Informação e Comunicações, especialmente no tocante ao monitoramento da segurança corporativa, à expedição de normas de segurança da informação, à realização de reuniões periódicas, com registro de deliberações em ata, e a outras atribuições correlatas constantes da mencionada IN;

—

Acórdão 592/2011 Plenário

9.1.2 em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VI, c/c a Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.3, institua Comitê de Segurança da Informação e Comunicações, observando as práticas contidas na NBR ISO/IEC 27002, item 6.1.2 Coordenação de segurança da informação;

9.1.5 em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, IV e art. 7º, c/c a Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.2, nomeie Gestor de Segurança da Informação e Comunicações, observando as práticas contidas na NBR ISO/IEC 27002, item 6.1.3 Atribuição de responsabilidade para segurança da informação;

ORGANIZAÇÃO INTERNA
(Textos extraídos de itens do Acórdão)

Acórdão 380/2011 Plenário	9.2.2 (...) monitore o funcionamento do comitê gestor de segurança e tecnologia da informação – CSTI de maneira a que este exerça suas atribuições; 9.2.6 em atenção ao disposto na Instrução Normativa – GSI/PR 1/2008, art. 5º, IV, e art. 7º, c/c a Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.2, nomeie gestor de segurança da informação e comunicações, com observância das práticas contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;
	—
Acórdão 2938/2010 Plenário	9.1.11 – em atenção ao artigo 13 da Resolução/CNJ nº 90/2009, institua Comitê de Segurança da Informação e Comunicações, observando as práticas contidas na NBR ISO/IEC 27002, item 6.1.2 – Coordenação de segurança da informação; 9.2.6 – em atenção ao princípio constitucional da eficiência, nomeie Gestor de Segurança da Informação, observando as práticas na NBR ISO/IEC 27002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação (item 3.14);
	—
Acórdão 2746/2010 Plenário	9.1.5 institua Comitê de Segurança da Informação e Comunicações, com observância da NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação, em atenção à IN GSI/PR 01/2008, art. 5º, VI, e à Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.3; 9.1.6 nomeie gestor de segurança da informação e comunicações, com observância da NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação, em atenção à IN GSI/PR 01/2008, art. 5º, IV, e art. 7º e à Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.2;

Organização interna
(Textos extraídos de itens do Acórdão)

Acórdão 1382/2009 Plenário	9.2 (...) envide esforços para que a [Área de TI] do Ministério seja dotada de servidores ocupantes de cargos efetivos em número suficiente, capacitados e treinados para exercer atividades estratégicas e sensíveis, sobretudo as que possam comprometer a segurança da tecnologia da informação do órgão, implantando controles compensatórios quando houver necessidade de que estas atividades sejam executadas por terceiros, à semelhança das orientações contidas na NBR ISO/IEC 17799:2005, item 6.1.3 - Atribuição de responsabilidades para a segurança da informação, e no Cobit 4.1, PO4.13 - Pessoal chave de TI;
	—
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 [Sistema], 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;

Organização interna
(Textos extraídos de itens do Acórdão)

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;

Partes externas
(Textos extraídos de itens do Acórdão)

Acórdão 2938/2010 Plenário

9.3 alertar [o Órgão] quanto à:

9.3.4 – não estabelecimento, nos editais e contratos de prestação de serviços de TI, de níveis mínimos de serviço a serem cumpridos pelas empresas contratadas, a fim de se resguardar quanto ao não cumprimento de padrões mínimos, disponibilidade, performance e incidência de erros, entre outros, decorrente do descumprimento da Lei nº 8.666/1993, art. 6º, inciso IX bem como do subitem 9.4.3 do Acórdão nº 786/2006 – Plenário;

9.3.7 – ausência de cláusula de sigilo, no Contrato (...), sobre o conteúdo de programas de computadores (fontes e executáveis), documentação e bases de dados, bem como a responsabilização pelo uso indevido dos equipamentos ou divulgação não autorizada dos dados e o período durante o qual subsistirão as obrigações de se manter sigilo "decorrente do descumprimento dos Acórdãos Plenários nos 71/2007, subitem 9.2.21 e 2023/2005, subitem 9.1.13.5;

Partes externas
(Textos extraídos de itens do Acórdão)

Acórdão 2746/2010 Plenário

9.3 alertar [o Órgão] quanto à:

3. insuficiência de cláusulas contratuais, decorrente do descumprimento do item 6.2.3 – "identificando segurança da informação nos acordos com terceiros" da NBR 27002 e do art. 12, II, da IN SLTI/MPOG 04/2008;

—

Acórdão 669/2008 Plenário

9.1.4 institua no âmbito da Coordenação-Geral de Informática e Telecomunicações políticas e procedimentos padronizados para monitorar as atividades dos terceirizados, à semelhança das orientações contidas nos itens 6.1.3, 6.2.3, 8.1.1, 8.1.3 e 10.2 da norma para segurança da informação, NBR ISO/IEC 17799:2005, e no item 4.14 do Cobit 4.1 (Políticas e procedimentos para terceirizados);

—

Acórdão 71/2007 Plenário

9.2.21 formalize, junto à [Agência de TI do Estado], um termo de compromisso que contemple de maneira específica a cópia das bases de dados do [Sistema] 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;

Partes Externas
(Textos extraídos de itens do Acórdão)

Acórdão 1663/2006 Plenário	9.2.3 elabore o acordo de nível de serviço do [Sistema];
	—
Acórdão 914/2006 Plenário	9.1.1 firmem contrato com relação ao [Programa de Governo], devendo ser estabelecida nesse instrumento cláusula que disponha sobre a propriedade intelectual de programas, documentação técnica e dados do [Sistema];
	9.3.1. firmem Acordo de Nível de Serviço, ou documento correlato, em relação ao [Sistema], 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;
	↘

Partes Externas
(Textos extraídos de itens do Acórdão)

Acórdão 914/2006 Plenário (continuação)

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;

↘

Partes Externas
(Textos extraídos de itens do Acórdão)

Acórdão 2023/2005 Plenário (continuação)

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;

↘

Partes Externas
(Textos extraídos de itens do Acórdão)

Acórdão 2023/2005 Plenário (continuação)

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 [Sistema];

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

4.7 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 instituição, além de assegurar que a informação seja classificada de acordo com o 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.

4.7.1 Que órdãos do TCU tratam, entre outros aspectos, da "Gestão de ativos"?

Responsabilidade pelos ativos
(Textos extraídos de itens do Acórdão)

Acórdão 1233/2012 Plenário	9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8): 9.15.12.5. processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;
	—
Acórdão 758/2011 Plenário	9.1.6 – aperfeiçoe o procedimento de inventário de ativos de informação, de maneira a que todos os ativos de informação estejam inventariados e tenham um proprietário responsável, à semelhança das orientações do item 7.1 da NBR ISO/IEC 27.002;

Responsabilidade pelos ativos
(Textos extraídos de itens do Acórdão)

Acórdão 757/2011 Plenário	9.2.8. em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VII, c/c Norma Complementar IN01/DSIC/GSIPR 4, item 5.2.1, estabeleça procedimento de inventário de ativos de informação, de maneira a que todos os ativos de informação sejam inventariados e tenham um proprietário responsável, com observância das práticas do item 7.1 da NBR ISO/IEC 27.002;
	—
Acórdão 381/2011 Plenário	9.1.15. (...) aperfeiçoe o procedimento de inventário de ativos de informação, de maneira a que todos os ativos de informação (dados, *hardware*, *software* e instalações) estejam inventariados e tenham um proprietário responsável, à semelhança das orientações contidas nas Normas Técnicas – NBR – ISO/IEC 27002, item 7.1.1 – Inventário de ativos e Gabinete de Segurança Institucional – Presidência da República – Norma Complementar 04/IN01/DSIC/GSIPR, item 5.2.1, conforme tratado no achado 13 – Falhas no inventário dos ativos de informação – do relatório de fiscalização;
	—
Acórdão 2938/2010 Plenário	9.1.13 – em atenção ao disposto na Resolução nº 90/2009, CNJ, art. 9º, § 2º, estabeleça processo de gestão de ativos de informação, de maneira que todos os ativos de informação sejam inventariados e tenham um proprietário responsável, observando as práticas contidas no item 7.1 da NBR ISO/IEC 27002;

Responsabilidade pelos ativos
(Textos extraídos de itens do Acórdão)

Acórdão 2746/2010 Plenário	9.1.10. estabeleça procedimento de inventário de ativos de informação, de maneira a que todos os ativos de informação sejam inventariados e tenham um proprietário responsável, com observância do item 7.1 da NBR ISO/IEC 27.002, em atenção à IN GSI/PR 01/2008, art. 5º, VII, e à Norma Complementar 04/IN01/DSIC/GSIPR, item 5.2.1;
	—
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 [Sistema], 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 [Sistema1], e futuramente, do sistema [Sistema2]; 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;

Classificação da informação
(Textos extraídos de itens do Acórdão)

Acórdão 1233/2012 Plenário	9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8): 9.15.12.6. processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II e art. 67;
	—
Acórdão 1137/2012 2ª Câmara	1.4.1.3. em atenção ao disposto no Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67, implante controles no Sistema Informatizado (...) em função da classificação da informação tratada no âmbito do [Programa de Governo];
	—
Acórdão 465/2011 Plenário	9.1.4. em atenção ao Decreto 4.553/2002, art. 6º, § 2º, II, e art. 67, crie critérios de classificação de informações, a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, com observância das práticas contidas no item 7.2 da NBR ISO/IEC 27.002;

Classificação da informação
(Textos extraídos de itens do Acórdão)

Acórdão 381/2011 Plenário	9.1.14. (...) implemente o prescrito no art. 6º da sua Política de Segurança da Informação, criando critérios de classificação das informações, a fim de que elas possam ter tratamento diferenciado em termos de seu valor, requisitos legais, grau de sensibilidade, grau de criticidade e necessidade de compartilhamento, considerando o teor do Decreto 4.553/2002, art. 6º, § 2º, I e II, e art. 67, e observando as práticas contidas no item 7.2 da Norma Técnica – NBR – ISO/IEC 27002, item 7.2 – Classificação da informação, conforme tratado no achado 14 – Inexistência de classificação da informação – do relatório de fiscalização;
	—
Acórdão 7312/2010 2ª Câmara	1.4.1.7. em atenção ao disposto no Decreto nº 4.553/2002, art. 6º, § 2º, inciso II e art. 67, crie critérios de classificação das informações a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, observando as práticas contidas no item 7.2 da NBR ISO/IEC 27.002 (Achado "Inexistência de classificação da informação");
	—
Acórdão 2938/2010 Plenário	9.2.5. – em consonância com o princípio constitucional da eficiência, estabeleça critérios de classificação das informações, a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, observando o disposto no item 7.2 (Classificação da informação) da NBR ISO/IEC nº 27002 e no item PO2.3 (Esquema de Classificação de Dados) do Cobit 4.1 (item 3.13);

Classificação da informação
(Textos extraídos de itens do Acórdão)

Acórdão 2746/2010 Plenário	9.1.9. crie critérios de classificação das informações, a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, com observância do item 7.2 da NBR ISO/IEC 27.002, em atenção ao Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67;
	—
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 [Sistema];

Classificação da informação
(Textos extraídos de itens do Acórdão)

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;

4.8 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 instituição. 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.

4.8.1 Que acórdãos do TCU tratam, entre outros aspectos, da "Segurança de recursos humanos"?

(Textos extraídos de itens do Acórdão)

Acórdão 669/2008 Plenário

9.1.4. institua no âmbito da Coordenação-Geral de Informática e Telecomunicações políticas e procedimentos padronizados para monitorar as atividades dos terceirizados, à semelhança das orientações contidas nos itens 6.1.3, 6.2.3, 8.1.1, 8.1.3 e 10.2 da norma para segurança da informação, NBR ISO/IEC 17799:2005, e no item 4.14 do Cobit 4.1 (Políticas e procedimentos para terceirizados);

—

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;

4.9 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 instituição. 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 instituição, reutilização e alienação segura de equipamentos, e, por fim, remoção de propriedade.

4.9.1 *Que acórdãos do TCU tratam, entre outros aspectos, da "Segurança física e do ambiente"?*

Áreas seguras
(Textos extraídos de itens do Acórdão)

Acórdão 1722/2008 Plenário

9.1.1.17. adote medidas para garantir que os recursos redundantes não estejam sujeitos aos mesmos riscos físicos e ambientais que os recursos principais, em conformidade com o previsto no item 9.1.4-b da ABNT NBR ISO/IEC 17799:2005;

9.1.1.18. estabeleça mecanismos de controle de acesso específico ao ambiente operacional do sistema (...), de acordo com o previsto no item 9.1 da ABNT NBR ISO/IEC 17799:2005;

Áreas seguras
(Textos extraídos de itens do Acórdão)

Acórdão 71/2007 Plenário	9.2.17. estabeleça um perímetro de segurança nas instalações da gerência do [Sistema] (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 [Sistema] 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;

Áreas seguras
(Textos extraídos de itens do Acórdão)

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;

Segurança de equipamentos
(Textos extraídos de itens do Acórdão)

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;

4.10 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.

4.10.1 *Que acórdãos do TCU tratam, entre outros aspectos, do "Gerenciamento das operações e comunicações"?*

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.2.1. ao estabelecer os procedimentos formais de gestão de mudanças, em atendimento ao item 9.1.7 do Acórdão 757/2011-TCU-Plenário, inclua controles para garantir que as mudanças implementadas no ambiente de produção dos sistemas sejam precedidas de homologação pelo gestor, observando ainda os itens 10.1.2, letra "d", e 12.5.1, letra "f", da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
	—
Acórdão 1382/2009 Plenário	9.2. (...) envide esforços para que sejam estabelecidos procedimentos com vistas a implementar a segregação de funções e assegurar sua efetividade na execução das atividades de tecnologia de informação, com base nas orientações contidas na NBR ISO/IEC 17799:2005, item 10.1.3 - Segregação de funções e no Cobit 4.1, item PO4.11 - Segregação de funções;
	—
Acórdão 309/2009 Plenário	9.1.37. segregue as funções e responsabilidades dos envolvidos com desenvolvimento e produção, em conformidade com o disposto no item 10.1.3 da NBR ISO/IEC 17799:2005;
	—
Acórdão 914/2006 Plenário	9.5.3. providencie a implantação do [Sistema] em ambiente de homologação dedicado a essa finalidade;

Procedimentos e responsabilidades operacionais
(Textos extraídos de itens do Acórdão)

Acórdão 562/2006 Plenário

9.2.2. elabore e distribua a todas as [Centrais] 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;

Procedimentos e responsabilidades operacionais
(Textos extraídos de itens do Acórdão)

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;

Gerenciamento de serviços terceirizados
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.3. estabeleça controles que permitam o monitoramento e análise crítica dos serviços de comunicação de dados contratados para atender às necessidades do [Programa de Governo], em especial dos *links* da Internet, com o objetivo de assegurar o cumprimento das definições de níveis de serviço por parte da empresa contratada, observando as recomendações do item 10.2.2 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

—

Acórdão 669/2008 Plenário

9.1.4. institua no âmbito da Coordenação-Geral de Informática e Telecomunicações políticas e procedimentos padronizados para monitorar as atividades dos terceirizados, à semelhança das orientações contidas nos itens 6.1.3, 6.2.3, 8.1.1, 8.1.3 e 10.2 da norma para segurança da informação, NBR ISO/IEC 17799:2005, e no item 4.14 do Cobit 4.1 (Políticas e procedimentos para terceirizados);

Planejamento e aceitação dos sistemas
(Textos extraídos de itens do Acórdão)

Acórdão 906/2009 Plenário	9.3.13. estabeleçam, de forma conjunta, e formalizem processo de homologação de novas versões e funcionalidades dos sistemas (...) utilizado pelos municípios e (...), à semelhança das orientações contidas nos itens 10.3.2 e 12.5.1 da NBR ISO/IEC 27002:2005, bem como no item AI7.7 do Cobit 4.1;
	—
Acórdão 309/2009 Plenário	9.1.28. defina procedimento formal para monitorar a utilização do sistema (...) e fazer projeções de necessidades de capacidade futura, para evitar potenciais gargalos e garantir o desempenho do sistema, em conformidade com o item 10.3.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações previstas nos itens AI3 e ME1 do Cobit 4.1;
	—
Acórdão 1722/2008 Plenário	9.1.1.10. estabeleça critérios formais para homologação e aceitação de atualizações e novas versões do sistema (...), de acordo com o previsto no item 10.3.2 da ABNT NBR ISO/IEC 17799:2005;
	—
Acórdão 71/2007 Plenário	9.2.13. estabeleça critérios formais para homologação e aceitação de atualizações e novas versões do [Sistema], 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 [Sistema];

Planejamento e aceitação dos sistemas
(Textos extraídos de itens do Acórdão)

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 [Sistema] pelo agente operador;

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

Cópias de segurança
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.8. defina e formalize uma política de cópias de segurança (*backups*) que inclua o código-fonte e a base de dados do [Sistema] com base nas necessidades de negócio do [Programa de Governo], incluindo procedimentos regulares de recuperação e observando as recomendações contidas no item 10.5.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

1.4.2.9. considerando a necessidade de proteger o sigilo das informações (...), avalie a conveniência de criptografar os dados gravados nas mídias das cópias de segurança do [Sistema], conforme recomenda a diretriz para implementação "h" do item 10.5.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

—

Acórdão 1382/2009 Plenário

9.2. (...) elabore e implante uma Política de Cópias de Segurança na Coordenação-Geral de Modernização e Informática em conformidade com as necessidades do negócio e com o Plano de Continuidade de Negócio a ser elaborado pelo órgão, em consonância com as orientações contidas na NBR ISO/IEC 17799:2005, item 10.5.1 - Cópia de segurança das informações e no Cobit 4.1, item DS11.5 - *Backup* e restauração;

Cópias de segurança
(Textos extraídos de itens do Acórdão)

Acórdão 669/2008 Plenário

9.4.7. elabore e implante uma Política de Cópias de Segurança, no âmbito da Coordenação-Geral de Informática e Telecomunicações (...), em conformidade com as necessidades do negócio, com o Plano de Continuidade de Negócio a ser elaborado pelo órgão e com as orientações contidas no item 10.5.1 da NBR ISO/IEC 17799:2005 e no item DS11.5 do Cobit 4.1 (*Backup* e restauração);

—

Acórdão 71/2007 Plenário

9.2.15. formalize política de geração de cópias de segurança para o [Sistema], 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 [Sistema] em local diverso da operação do sistema, de acordo com a diretriz "d" do item 10.5.1 da NBR ISO/IEC 17799:2005;

Manuseio de mídias
(Textos extraídos de itens do Acórdão)

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;

Manuseio de mídias
(Textos extraídos de itens do Acórdão)

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;

Troca de informações
(Textos extraídos de itens do Acórdão)

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;

Serviços de comércio eletrônico
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.13. na proteção da confidencialidade do tráfego de rede para utilização do [Sistema], utilize recursos de criptografia, observando a Norma Complementar - IN01/DSIC/GSI/PR 9/2010 e ainda as orientações dos itens 10.9.2, diretriz para implementação "c", 11.5.1, diretriz para implementação "i", e 12.3.1, todos da Norma Técnica ABNT NBR ISO/IEC 27002:2005.

Monitoramento
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.4. implante mecanismos de proteção dos registros de auditoria (*logs*) contra modificações e exclusões não autorizadas, em especial por parte de usuários administradores, bem como contra problemas operacionais, observando as recomendações do item 10.10.3 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

1.4.2.5. implante procedimentos que possibilitem o monitoramento proativo do uso dos recursos de infraestrutura de TI que dão suporte ao [Sistema], observando as recomendações do item 10.10.2 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

1.4.2.6. implante controle formal (motivação, aprovação e documentação), registros de auditoria (*logs*), monitoramento e análise crítica regular das atividades de usuários administradores, observando as recomendações do item 10.10.4 da Norma Técnica ABNT NBR ISO/IEC 27002:2005, ou implante controles compensatórios para monitorar as atividades realizadas por estes usuários;

↘

Monitoramento
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara (continuação)	1.4.3.3. em atenção ao disposto no item 5.3.4 da Norma Complementar - IN 01/DSIC/GSI/PR 7/2010, defina todas as alterações relevantes no [Sistema] (...) e adote medidas para que o sistema registre essas alterações, definindo, ainda, por quanto tempo o sistema manterá esses registros, observando as diretrizes contidas no item 10.10.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
	—
Acórdão 906/2009 Plenário	9.3.7. implementem procedimento para controlar as informações alteradas pelo usuário do sistema (...) utilizado pelos municípios, registrando a sequência de ações executadas por ele no sistema, com vistas a viabilizar a realização de auditorias para identificar e responsabilizar os causadores de possíveis danos aos dados municipais, à semelhança do item 10.10.1 da NBR ISO/IEC 27002:2005;
	—
Acórdão 309/2009 Plenário	9.1.38. mantenha ativado o registro (*log*) das operações de acesso direto ao banco de dados feitas pelos administradores e desenvolvedores do sistema (...), em conformidade com o item 10.10.4 da NBR ISO/IEC 17799:2005;
	9.1.39. adote procedimento formal e automatizado para acesso aos *logs* das transações do sistema (...), de forma a não haver dependência dos desenvolvedores e não haver consultas diretas no banco de dados, com base nas diretrizes previstas nos itens 10.10.1 e 10.10.2 da NBR ISO/IEC 17799:2005;

	Monitoramento (Textos extraídos de itens do Acórdão)
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 [Sistema] 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 [na Base de Dados do Sistema], 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 [Sistema], 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 [Sistema], as informações relativas às alterações efetuadas;

Monitoramento
(Textos extraídos de itens do Acórdão)

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 (...) 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 (...); 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 planejamento de segurança do sistema de pagamento de pessoal [...], a análise regular e sistemática dos registros (*logs*) de sistema operacional e do próprio sistema de pagamento; 9.2.3. utilize, preferencialmente, ferramentas de auditoria, como *softwares* especializados, na análise dos registros (*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;

4.11 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, ao sistema operacional, à aplicação e à 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.

4.11.1 Que acórdãos do TCU tratam, entre outros aspectos, do "Controle de acessos"?

Requisitos de negócio para controle de acesso
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.3.1. em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VII, **in fine**, e à Norma Complementar - IN01/DSIC/GSI/PR 7/2010, item 2.6, defina uma Política de Controle de Acesso (PCA) contemplando os ativos de informação do [Programa de Governo], em especial o [Sistema], observando as diretrizes da Norma Complementar - IN01/DSIC/GSI/PR 7/2010, e ainda as orientações contidas no item 11.1.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
	—
Acórdão 2831/2011 Plenário	9.2.3. em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VII, in fine, e à Norma Complementar 07/IN01/DSIC/GSI/PR, item 2.6, defina política de controle de acesso a informações e recursos de TI, com base nos requisitos de negócio e de segurança da informação da entidade, com observância das orientações do item 11.1.1 da NBR ISO/IEC 27002:2005 (achado 2.2 do relatório de auditoria);

Requisitos de negócio para controle de acesso
(Textos extraídos de itens do Acórdão)

Acórdão 1382/2009 Plenário	9.2. (...) defina e implante uma Política de Controle de Acesso (PCA) para toda a organização, nos termos das orientações contidas NBR ISO/IEC 17799:2005, item 11.1.1 - Política de controle de acesso e à semelhança das orientações contidas no Cobit 4.1, itens DS5.3 - Gestão de identidades e DS5.4 - Gestão de contas de usuários;
	—
Acórdão 906/2009 Plenário	9.3.2. definam política de controle de acesso ao sistema (...) utilizado pelos municípios, em consonância com as orientações do item 11.1.1 da NBR ISO/IEC 27002:2005;
	—
Acórdão 309/2009 Plenário	9.1.30. elabore, aprove formalmente, divulgue e implemente política de controle de acesso, conforme item 11.1.1 da NBR ISO/IEC 17799:2005;
	—
Acórdão 669/2008 Plenário	9.4.6. defina e implante uma Política de Controle de Acesso (PCA) para toda a organização, nos termos das orientações contidas no item 11.1.1 da NBR ISO/IEC 17799:2005 e em harmonia com as diretrizes expostas nos itens DS 5.3 e DS 5.4 do Cobit 4.1 (Gestão de identidades e Gestão de contas de usuários);
	—
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;

Requisitos de negócio para controle de acesso
(Textos extraídos de itens do Acórdão)

Acórdão 71/2007 Plenário

9.2.7. defina formalmente uma Política de Controle de Acesso - PCA - para o [Sistema], contemplando usuários Web, "*host* de atualização" e da rede interna da gerência do [Sistema], 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:

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.7. utilize contas de usuários únicas, pessoais e não compartilhadas de forma a possibilitar a identificação dos autores de atividades realizadas com privilégios administrativos no sistema operacional e no banco de dados, conforme recomendado no item 11.2.1, diretriz para implementação "a", da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

1.4.3.2. em atenção ao disposto no item 5.1 da Norma Complementar - IN01/DSIC 7/2010 do Gabinete de Segurança Institucional da Presidência da República, formalize procedimentos de gerenciamento de acesso de usuários de modo a assegurar o acesso devidamente autorizado às informações restritas do [Sistema], observando ainda as recomendações contidas no item 11.2 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

Acórdão 2831/2011 Plenário

9.2.2. em atenção à Norma Complementar 07/IN01/DSIC/GSI/PR, item 5.1, implante processos formais de registro de usuário, gerenciamento de senhas, gerenciamento de privilégios e análise crítica dos direitos de acesso, com vistas a garantir efetividade dos procedimentos de controle de acesso operacionalizados para esses processos, com observância das recomendações do item 11.2 e subitens da NBR ISO/IEC 27002:2005 (achado 2.2 do relatório de auditoria);

9.2.9.2. avalie perfis dos usuários (...) e, se for o caso, adote as providências necessárias para torná-las compatíveis com as regras as regras de segregação de funções (achado 2.6 do relatório de auditoria);

9.2.9.3. implante controles no [Sistema] capazes de impedir concessão de perfis de usuários em desacordo com as regras de segregação de funções definidas e de obstar a realização de operações em desacordo com essas regras, à semelhança do controle de aplicação AC1 do COBIT 4.1 (achado 2.6 do relatório de auditoria);

9.2.10. em atenção à Norma Complementar 07/IN01/DSIC/GSI/PR, item 2.2, avalie perfis de usuários existentes (...) e, se for o caso, adote as providências necessárias para torná-los compatíveis com as regras definidas no processo de trabalho formalmente estabelecido (achado 2.7 do relatório de auditoria);

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

Acórdão 2812/2009 Plenário	9.1.16. com base na NBR ISO/IEC 27002:2005, item 11.2.4.a, estabeleça procedimentos de revisão periódica de direitos de acesso dos usuários (...);
	9.1.17. com base na NBR ISO/IEC 27002:2005, itens 11.2.1.h e 11.2.4.a, institua procedimento automático de revogação do acesso de usuários após período pré-definido de inatividade (...);
	—
Acórdão 906/2009 Plenário	9.3.3 implementem procedimento para bloquear usuários inativos por um período de tempo predeterminado no controle de acesso aos sistemas (...) utilizado pelos municípios, (...) à semelhança do item 11.2.1 da NBR ISO/IEC 27002:2005;
	9.3.8. apresentem ao usuário cadastrado nos sistemas (...) declaração por escrito com os direitos de acesso dele, à semelhança do item 11.2.1 da NBR ISO/IEC 27002:2005;
	—
Acórdão 309/2009 Plenário	9.1.31. defina Processo de autorização formal para concessão e revogação de acesso, conforme item 11.2.2 da NBR ISO/IEC 17799:2005;
	9.1.32. torne obrigatória, no Processo de concessão de acesso, a assinatura de termo de compromisso pelos usuários do sistema (...), conforme item 11.2.1, alíneas "d" e "e" da NBR ISO/IEC 17799:2005;
	9.1.34. defina formalmente política de gerenciamento das senhas dos usuários do sistema DOF e adote sistema que assegure a sua qualidade, conforme itens 11.2.3 e 11.5.3 da NBR ISO/IEC 17799:2005;

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

Acórdão 71/2007 Plenário	9.2.8. conduza, a intervalos regulares, a análise crítica dos direitos de acesso dos usuários do [Sistema], 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 [Sistema] (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 [Sistema] 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;

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

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 preveem 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;

Gerenciamento de acesso do usuário
(Textos extraídos de itens do Acórdão)

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;

Responsabilidades dos usuários
(Textos extraídos de itens do Acórdão)

Acórdão 906/2009 Plenário

9.3.4. implementem procedimento de revisão e alteração periódica de senha para os sistemas CadÚnico utilizado pelos municípios, (...) à semelhança do item 11.3.1 da NBR ISO/IEC 27002:2005;

9.3.5. implementem procedimento para verificação da qualidade das senhas digitadas pelos usuários do sistema [Sistema] utilizado pelos municípios, à semelhança do item 11.3.1 da NBR ISO/IEC 27002:2005;

9.3.9. incluam orientações nas páginas de acesso aos sistemas (...) de como o usuário pode alterar sua senha, com vistas a assegurar a efetividade da diretriz estabelecida no item 11.3.1 da NBR ISO/IEC 27002:2005;

—

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;

Responsabilidades dos usuários
(Textos extraídos de itens do Acórdão)

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;

Controle de acesso à rede
(Textos extraídos de itens do Acórdão)

Acórdão 309/2009 Plenário	9.1.35. defina formalmente política de uso dos serviços de rede, conforme item 11.4.1 da NBR ISO/IEC 17799:2005; 9.1.36. adote controle de acesso à rede, conforme item 11.4.6 da NBR ISO/IEC 17799:2005;

Controle de acesso ao sistema operacional
(Textos extraídos de itens do Acórdão)

Acórdão 906/2009 Plenário	9.3.6. implementem procedimento para bloquear usuários após várias tentativas de autenticação com senhas inválidas no controle de acesso dos sistemas (...) utilizado pelos municípios, (...) à semelhança do item 11.5.1 da NBR ISO/IEC 27002:2005;
	—
Acórdão 09/2009 Plenário	9.1.33. estabeleça procedimentos seguros de entrada no sistema operacional das estações de trabalho e no sistema DOF, conforme item 11.5.1 da NBR ISO/IEC 17799:2005;
	—
Acórdão 71/2007 Plenário	9.2.26. estabeleça procedimentos formais para a execução de operações diretamente sobre as bases de dados do [Sistema] 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;

Controle de acesso ao sistema operacional
(Textos extraídos de itens do Acórdão)

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 [Sistema], após a entrada no Sistema com sucesso, a apresentação das informações ao usuário da data e hora de última entrada válida no [Sistema]; 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;

Controle de acesso à aplicação e à informação
(Textos extraídos de itens do Acórdão)

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;

4.12 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.

4.12.1 Que acórdãos do TCU tratam, entre outros aspectos, da "Aquisição, desenvolvimento e manutenção de sistemas de informação"?

Processamento correto nas aplicações
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.4.2. aperfeiçoe as críticas de entrada de dados do [Sistema], para mitigar os riscos de incorreção, (...) observando as orientações contidas no item 12.2.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

Processamento correto nas aplicações
(Textos extraídos de itens do Acórdão)

Acórdão 1722/2008 Plenário	9.1.1.2. continue a executar alterações no sistema (...), para validação de dados de entrada, controle do processamento interno de dados e validação de dados de saída, em conformidade com o previsto nos itens 12.2.1, 12.2.2 e 12.2.4 da ABNT NBR ISO/IEC 17799:2005; 9.1.1.3. aperfeiçoe o tratamento de exceções do sistema (...), a validação de dados de entrada e o controle do processamento interno, em conformidade com a especificação de requisitos do sistema e com os itens 12.2.1 e 12.2.2 da ABNT NBR ISO/IEC 17799:2005;
	—
Acórdão 71/2007 Plenário	9.2.3. institua mecanismos que garantam a consistência entre [as bases de dados], verificando periodicamente a eficácia dos mecanismos implementados, de acordo com o previsto no item 12.2.2, da NBR ISO/IEC 17799:2005;

Controles criptográficos
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.2.13. na proteção da confidencialidade do tráfego de rede para utilização do [Sistema], utilize recursos de criptografia, observando a Norma Complementar - IN01/DSIC/GSI/PR 9/2010 e ainda as orientações dos itens 10.9.2, diretriz para implementação "c", 11.5.1, diretriz para implementação "i", e 12.3.1, todos da Norma Técnica ABNT NBR ISO/IEC 27002:2005.
	—
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 (...) em suas futuras versões;

Segurança em processos de desenvolvimento e de suporte
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.2.1. ao estabelecer os procedimentos formais de gestão de mudanças, em atendimento ao item 9.1.7 do Acórdão 757/2011-TCU-Plenário, inclua controles para garantir que as mudanças implementadas no ambiente de produção dos sistemas sejam precedidas de homologação pelo gestor, observando ainda os itens 10.1.2, letra "d", e 12.5.1, letra "f", da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
	—
Acórdão 381/2011 Plenário	9.1.2. (...) estabeleça procedimentos formais de gestão de mudanças, à semelhança das orientações contidas na Norma Técnica – ITGI – Cobit 4.1, AI6 – Gerenciar mudanças e de outras reconhecidas práticas de mercado (como as Normas Técnicas – NBR – ISO/IEC 27002, item 12.5.1 – Procedimentos para controle de mudanças e NBR ISO/IEC 20000, item 9.2 – Gerenciamento de mudanças), conforme tratado no achado 11 – Inexistência do processo de gestão de mudanças – do relatório de fiscalização;
	—
Acórdão 111/2011 Plenário	9.1.7. estabeleça procedimentos formais de gestão de mudanças, de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 27.002, à semelhança das orientações contidas no Cobit 4.1, processo AI6 – Gerenciar mudanças e de outras boas práticas de mercado, como a NBR ISO/IEC 20.000;
	—
Acórdão 1382/2009 Plenário	9.2. (...) estabeleça, no âmbito da [Área de TI], procedimentos formais de controle de demandas e de mudanças, de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 17799:2005, à semelhança das orientações contidas no Cobit 4.1, processo AI6 - Gerenciar mudanças;

Segurança em processos de desenvolvimento e de suporte
(Textos extraídos de itens do Acórdão)

Acórdão 309/2009 Plenário	9.1.7. elabore procedimentos formais de controle de demandas e de mudanças, em concordância com o item 12.5.1 da NBR ISO/IEC 17799:2005;
	—
Acórdão 1722/2008 Plenário	9.1.1.9. estabeleça procedimentos formais de controle de mudanças no sistema (...), de acordo com o previsto no item 12.5.1 da ABNT NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas nos itens AI6 e AI6.2 do Cobit 4.1;
	—
Acórdão 669/2008 Plenário	9.4.3. em atenção ao Princípio da Eficiência, estabeleça procedimentos formais de controle de demandas e mudanças, de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 17799:2005, à semelhança das orientações contidas no item AI6 do Cobit 4.1 (Gerencia de Mudança);
	—
Acórdão 71/2007 Plenário	9.2.12.estabeleça procedimentos formais de controle de demandas e de mudanças no [Sistema], de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas no item AI6.2 do COBIT 4.0;
	—
Acórdão 1663/2006 Plenário	9.1.4. implemente sistemática de homologação e controle das versões implantadas do [Sistema];

Segurança em processos de desenvolvimento e de suporte
(Textos extraídos de itens do Acórdão)

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;

Gestão de vulnerabilidades técnicas
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara

1.4.2.10. aperfeiçoe os controles de vulnerabilidades técnicas para os recursos de infraestrutura de TI que dão suporte ao [Sistema], especialmente quanto à necessidade de que esses controles façam parte de um processo de gestão de mudanças, conforme recomenda o item 12.6.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

4.13 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.

4.13.1 Que acórdãos do TCU tratam, entre outros aspectos, da "Gestão de incidentes de segurança da informação"?

Notificação de fragilidades e eventos de segurança da informação

(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.2.11. na ocasião do cumprimento dos itens 9.1.5 e 9.2.6 do Acórdão 757/2011-TCU-Plenário, observe as recomendações dos itens 13.1.1. e 13.2.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005, incluindo canais apropriados de notificação por parte dos usuários do [Sistema] no processo de gestão de incidentes;
	—
Acórdão 71/2007 Plenário	9.1.3. implemente serviço de atendimento ao usuário do [Sistema] (*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);

Gestão de incidentes de segurança da informação e melhorias

(Textos extraídos de itens do Acórdão)

Acórdão 866/2011 Plenário	9.2.6. em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, V, institua equipe de tratamento e resposta a incidentes em redes computacionais, observando a Norma Complementar 05/IN01/DSIC/GSIPR;

Gestão de incidentes de segurança da informação e melhorias
(Textos extraídos de itens do Acórdão)

Acórdão 594/2011 Plenário

9.4.7. em atenção à IN GSI/PR 1/2008, art. 5º, V, reformule a atuação da equipe de tratamento e resposta a incidentes em redes computacionais, de maneira a atender às Normas Complementares 5/IN/01/DSIC/GSIPR e 8/IN/01/DSIC/GSI/PR, especialmente quanto à designação formal dos integrantes e ao tratamento de resposta a incidentes;

—

Acórdão 7312/2010 2ª Câmara

1.4.1.9. em atenção ao disposto na Instrução Normativa GSI/PR nº 01/2008, art. 5º, V, institua equipe de tratamento e resposta a incidentes em redes computacionais, observando as práticas contidas na Norma Complementar 05/IN01/DSIC/GSIPR (Achado "Inexistência de equipe de tratamento e resposta a incidentes em redes computacionais – ETRI");

—

Acórdão 2746/2010 Plenário

9.1.8 institua equipe de tratamento e resposta a incidentes em redes computacionais, com observância da Norma Complementar 05/IN01/DSIC/GSIPR, em atenção à IN GSI/PR 01/2008, art. 5º, V;

4.14 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 a 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 realizar análise e avaliação de riscos, além de desenvolver, implementar, testar e reavaliar planos de continuidade relativos à segurança da informação.

4.14.1 Que acórdãos do TCU tratam, entre outros aspectos, da "Gestão da continuidade do negócio"?

ASPECTOS DA GESTÃO DA CONTINUIDADE DO NEGÓCIO, RELATIVOS À SEGURANÇA DA INFORMAÇÃO
(Textos extraídos de itens do Acórdão)

Acórdão 1137/2012 2ª Câmara	1.4.1.2. em atenção à Norma Complementar - IN01/DSIC/GSI/PR 6/2009, implante um Programa de Gestão da Continuidade de Negócios adequado às necessidades do ministério, (...) observando ainda as diretrizes presentes no item 14 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;
	—
Acórdão 1382/2009 Plenário	9.2. (...) defina formalmente um Plano de Continuidade do Negócio (PCN) que garanta, em caso de falhas ou desastre natural significativo, a retomada tempestiva do funcionamento do órgão, protegendo os processos críticos, de acordo com o previsto no item 14 da NBR ISO/IEC 17799:2005, e segundo orientações contidas no Cobit 4.1, item DS4.2 - Planos de Continuidade de TI;
	—
Acórdão 1722/2008 Plenário	9.1.1.11. defina plano formal de contingência dos ativos de informática do sistema (..), contemplando o disposto no item 14 da ABNT NBR ISO/IEC 17799:2005, assegurando que esse plano seja testado e atualizado regularmente, conforme o previsto no item 14.1.5 da ABNT NBR ISO/IEC 17799:2005; 9.1.1.12. promova atividades de treinamento, conscientização e educação sobre o plano de contingência que vier a ser adotado, em conformidade com a diretriz "g" do item 14.1.4 da ABNT NBR ISO/IEC 17799:2005;

Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
(Textos extraídos de itens do Acórdão)

Acórdão 669/2008 Plenário	9.4.4. defina formalmente um Plano de Continuidade do Negócio (PCN) que garanta, em caso de falhas ou desastre natural significativo, a retomada tempestiva do funcionamento do órgão e proteja os processos críticos, de acordo com o previsto no item 14 da NBR ISO/IEC 17799:2005 e segundo as orientações contidas no item DS4.2 do Cobit 4.1 (Planos de Continuidade de TI);
	—
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 [Sistema], 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 [...];

Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
(Textos extraídos de itens do Acórdão)

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 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;
	—
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;

4.15 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.

4.15.1 Que acórdãos do TCU tratam, entre outros aspectos, da "Conformidade"?

Conformidade com requisitos legais
(Textos extraídos de itens do Acórdão)

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
(Textos extraídos de itens do Acórdão)

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;

Considerações quanto à auditoria de sistemas de informações
(Textos extraídos de itens do Acórdão)

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;

5 Referências

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120p.

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.

DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Books, 2000. 218p.

Responsabilidade pelo conteúdo

Secretaria de Fiscalização de Tecnologia da Informação
Secretaria-Geral de Controle Externo

Elaboração

Cláudia Augusto Dias
Roberta Ribeiro de Queiroz Martins

Atualização

Maurício Laurentino de Mesquita
Roberta Ribeiro de Queiroz Martins
Sylvio Xavier Junior

Responsabilidade editorial

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

Projeto gráfico, diagramação e capa

Paulo Brandão

Foto da capa

Pakize Öztürk (stock.xchng)

Tribunal de Contas da União

Secretaria de Fiscalização de Tecnologia da Informação
SAFS Quadra 4 Lote 1
Anexo I sala 311
70.042-900 Brasília - DF
(61) 3316 5371
Fax (61) 3316 5372
sefti@tcu.gov.br

Ouvidoria

Fone 0800 644 1500
Impresso pela Sesap/Segedam

Negócio

Controle externo da Administração Pública e da gestão dos recursos públicos federais

Missão

Controlar a Administração Pública para promover seu aperfeiçoamento em benefício da sociedade

Visão

Ser reconhecido como instituição de excelência no controle e no aperfeiçoamento da Administração Pública

www.tcu.gov.br