Instituto de Previdência e Assistência dos Servidores do Município de Vitória

Política de segurança da informação

PSI

Sumário

1- INTRODUÇÃO

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, "*A **informação** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente."*

De acordo com a mesma norma, *"**Segurança da informação** é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."*

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

Integridade: somente alterações, supressões e adições que forem autorizadas pela instituição devem ser realizadas nas informações;

Confidencialidade: somente pessoas devidamente autorizadas pela instituição devem ter acesso à informação;

Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

A violação desta política de segurança é qualquer ato que:

- Exponha o Instituto a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, *"A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."*

Mediante tal embasamento e considerando o disposto em seu Planejamento Estratégico, o IPAMV resolve implantar um Sistema de Segurança da Informação (S.S.I.), cuja estrutura e diretrizes são expressas neste documento.

2 - TERMOS E DEFINIÇÕES

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335-1:2004]

Ativo: qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004]

Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005]

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que

tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

Informação: agrupamento de dados que contenham algum significado.

Risco: combinação da probabilidade de um evento e de suas consequências. [ABNT ISO/IEC Guia 73:2005]

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005]

3 – OBJETIVO

O presente documento constitui uma declaração formal do IPAMV acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observado por todos os seus servidores, segurados, estagiários e prestadores de serviços.

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação na Instituição, estabelecendo as diretrizes a serem seguidas para implantação e manutenção de um S.S.I., guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

É dever de todos dentro do IPAMV:

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a instituição e deve sempre ser tratada profissionalmente.

4 - ESTRUTURA NORMATIVA

Os documentos que compõem a estrutura normativa são divididos em três categorias:

a) Política (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o IPAMV decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve

como base para que as normas e os procedimentos sejam criados e detalhados;

b) Normas (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política;

c) Procedimentos (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades do IPAMV.

4.1 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Os documentos integrantes da estrutura devem ser divulgados a todos os servidores, segurados, estagiários e prestadores de serviços do IPAMV quando de sua admissão, bem como, através dos meios oficiais de divulgação interna do IPAMV e, também, publicadas no site da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

4.2 APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação do IPAMV deverão ser aprovados e revisados conforme critérios descritos abaixo:

a) Política
Nível de aprovação: Diretoria Executiva
Periodicidade da revisão: anual

b) Normas
Nível de aprovação: Diretoria Executiva
Periodicidade da revisão: semestral

c) Procedimentos
Nível de aprovação: Diretoria responsável pela área envolvida.
Periodicidade da revisão: semestral.

Durante o primeiro ano de vigência de cada documento, considerado a partir da data de sua publicação, a periodicidade das revisões será igual à metade dos períodos acima definidos.

5 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da política de segurança da informação do IPAMV que constituem os principais pilares do sistema de segurança da informação da instituição, norteando a elaboração das normas e procedimentos.

5.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Define-se como necessária a classificação de toda a informação de propriedade do IPAMV, de maneira proporcional ao seu valor para a instituição, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

a) Pública: É uma informação do IPAMV ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

b) Interna: É uma informação do IPAMV o qual não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos ao IPAMV deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da instituição, porém, não com a mesma magnitude de uma informação confidencial ou restrita. Pode ser acessada sem restrições por todos os segurados e prestadores de serviços do IPAMV.

c) Confidencial: É uma informação crítica para os servidores do IPAMV ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, segurados e/ou fornecedores.

d) Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil

acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

5.2 PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, segurado, estagiário ou prestador de serviços do IPAMV, sendo que:

a) Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do IPAMV e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade do IPAMV;

b) As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

c) Assuntos confidenciais não devem ser expostos publicamente;

d) Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

e) Somente softwares homologados podem ser utilizados no ambiente computacional do IPAMV;

f) Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

g) Todo usuário, para poder acessar dados das redes de computadores do IPAMV, deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;

h) Não é permitido o compartilhamento de pastas nos computadores de servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

i) Todos os dados considerados como imprescindíveis aos objetivos do IPAMV devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

5.3 PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o IPAMV detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPAMV e reafirmam o seu compromisso com a melhoria contínua desse processo:

a) As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;

b) As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

c) As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;

d) As informações somente são fornecidas a terceiros, mediante autorização prévia da diretoria executiva ou para o atendimento de exigência legal ou regulamentar;

e) As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

6 - TRANSFERÊNCIAS DE SERVIDORES

Quando um servidor for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido servidor ao sistema informatizado do IPAMV.

7 - CÓPIAS DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do IPAMV.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IPAMV, o setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

8 - USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais no IPAMV. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o instituto não devem ser acessados.

Não é permitido instalar programas provenientes da Internet nos microcomputadores do IPAMV, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios do IPAMV;
- Que promovam discussão pública sobre os negócios do IPAMV, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

9 - USO DO CORREIO ELETRÔNICO – (E-mail)

O correio eletrônico fornecido pelo IPAMV é um instrumento de comunicação interna e externa do instituto. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do IPAMV, não podem ser contrárias à legislação vigente e nem aos princípios éticos. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas do IPAMV.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao setor de informática, que providenciará a inclusão do mesmo.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

Em caso de congestionamento no sistema de correio eletrônico, o setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou.

O setor de Informática poderá, visando evitar a entrada de vírus no IPAMV, bloquear o recebimento de e-mails provenientes de sites gratuitos.

10 - NECESSIDADES DE NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS

O setor de Informática é responsável pela aplicação da Política do IPAMV em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

11 - USO DE COMPUTADORES PESSOAIS (LAPTOPS) DE PROPIEDADE DO IPAMV

Os servidores que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do IPAMV, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao setor de Informática;
- Envie uma cópia da ocorrência para o setor de Informática.

12 - PAPÉIS E RESPONSABILIDADES

12.1 SERVIDORES, SEGURADOS, ESTAGIÁRIOS, E PRESTADORES DE SERVIÇOS.

Todo arquivo em mídia proveniente de entidade externa ao IPAMV deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Cabe aos servidores, estagiários e prestadores de serviços do IPAMV cumprir com as seguintes obrigações:

a) Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;

b) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;

c) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

d) Comunicar imediatamente ao setor de Informática qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

12.2 GESTOR DA INFORMAÇÃO

O Gestor da Informação é um servidor de TI sugerido pelo gerente de TI e designado pela Diretoria como responsável por um determinado ativo de informação.

Este gestor deve dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade do IPAMV.

O Gestor da Informação pode delegar sua autoridade sobre o ativo de informação, porém, continua sendo dele a responsabilidade final pela sua proteção.

Compete ao Gestor da Informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;

b) Inventariar todos os ativos de informação sob sua responsabilidade;

c) Enviar ao Gerente de TI, quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo Gerente de TI e aprovados pela Diretoria;

d) Sugerir procedimentos ao Gerente de TI para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;

e) Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;

f) Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

g) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

12.3 GERÊNCIAS

Cabe às Gerências:

a) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;

b) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

c) Sugerir ao Gestor, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;

d) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo Gestor;

e) Comunicar imediatamente ao Gestor eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

12.4 DIRETORIA JURÍDICA

Cabe, adicionalmente, à diretoria Jurídica:

a) Manter as áreas do IPAMV informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

b) Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do IPAMV;

c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

12.5 GERÊNCIA DE RECURSOS HUMANOS

Cabe, adicionalmente, à Gerência de Recursos Humanos:

a) Assegurar-se de que os servidores e estagiários, comprovem, por escrito, estarem cientes da estrutura normativa de segurança e dos documentos que as compõem;

b) Criar mecanismos para informar, antecipadamente aos fatos, alterações no quadro de servidores do IPAMV.

12.6 DIRETORIA EXECUTIVA

Cabe à Diretoria Executiva:

a) Aprovar a política e as normas de segurança da informação e suas revisões;

b) Nomear os gestores da informação, conforme as indicações do Gerente de TI;

d) Receber, por intermédio do setor de informática, relatórios de violações da política e das normas de segurança da informação, quando aplicáveis;

e) Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do setor de informática.

13 - AUDITORIA

Todo ativo de informação sob responsabilidade do setor de informática é passível de auditoria em data e horários determinados pelo Gestor, podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do IPAMV.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de Segurança da Informação poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

14 - VIOLAÇÕES E SANÇÕES

14.1 VIOLAÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a) Quaisquer ações ou situações que possam expor o IPAMV ou seus segurados à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b) Utilização indevida de dados da Instituição, divulgação não autorizada de informações, sem a permissão expressa do Gestor da Informação;

c) Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do IPAMV ou de seus segurados;

d) A não comunicação imediata à área de Gerencia da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um servidor, segurado, estagiário ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

14.2 SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação do IPAMV são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

15 - LEGISLAÇÃO APLICÁVEL

Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);

Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias).