PORTARIA N.º 437, DE 09 DE JUNHO DE 2020

*Dispõe sobre as **Normas Complementares de Segurança**.*

A SUPERINTENDÊNCIA DO SEPREV – Serviço de Previdência e Assistência à Saúde dos Servidores Municipais de Indaiatuba, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO o disposto no art. 7º da Resolução nº 327/2019, que aprova a Política de Segurança da Informação do SEPREV e delega à Superintendência a atribuição de estabelecer Normas Complementares de Segurança;

R E S O L V E:

Art. 1º. Aprovar as Normas Complementares de Segurança, em atendimento ao disposto no art. 7º da Resolução nº 327/2019 do Conselho Administrativo, conforme os seguintes Anexos desta Portaria:

Anexo I – NCS-01 – Serviço de Correio Eletrônico;
Anexo II – NCS-02 – Serviço de Internet;
Anexo III – NCS-03 – Computadores, Softwares e outros recursos de Tecnologia Da Informação;
Anexo IV – NCS-04 – Identificação e Controle de Acesso;
Anexo V – NCS-05 – Procedimentos de Contingência; e
Anexo VI – NCS-06 – Orientações específicas para os colaboradores lotados no Departamento de Tecnologia da Informação.

Art. 2º. Competirá ao Departamento de Tecnologia da Informação providenciar as ações necessárias para cumprimento das normas complementares aprovadas por esta Portaria, bem como a realização de ações de conscientização quanto à segurança da informação.

Art. 3º. Esta Portaria entrará em vigor nesta data.

Indaiatuba, 09 de junho de 2020.

Antonio Corrêa
Superintendente

ANEXO I – PORTARIA Nº 437/2020
NCS-01 - SERVIÇO DE CORREIO ELETRÔNICO
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Conceitos e Definições

1.1. Serviço de correio eletrônico – serviço de envio e recebimento de mensagens eletrônicas (também conhecidas por "e-mails") no âmbito do SEPREV.

1.2. Caixa Postal: conta de correio eletrônico onde são armazenadas as mensagens enviadas e recebidas. Cada colaborador tem um endereço eletrônico e uma caixa postal exclusivos.

1.3. Endereço eletrônico: conjunto de caracteres que individualiza e identifica o remetente e o destinatário de uma mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo caractere "@". Exemplo: identificador@seprev.sp.gov.br

1.4. Spam: termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

1.5. Malware: é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

1.6. Phishing: é o termo que designa as tentativas de obtenção de informação pessoal identificável através de uma suplantação de identidade por parte de criminosos em contextos informáticos.

1.7. Hoax: é uma tentativa de enganar um grupo de pessoas, fazendo-as acreditar que algo falso é real.

2. Caixas postais de correio eletrônico

2.1. O domínio adotado para a utilização de caixas postais eletrônicas do SEPREV é **@seprev.sp.gov.br**

2.2. A identificação dos colaboradores seguirá o padrão "**nome.sobrenome**" seguido do domínio @seprev.sp.gov.br.

2.3. A capacidade mínima das caixas postais será de, no mínimo, **30 GB** (trinta gigabytes).

2.4. Somente será criada caixa postal para servidores e estagiários do SEPREV, ou a fornecedores que estejam prestando serviços contínuos na sede da Autarquia.

2.5. As solicitações para criação de caixas postais deverão ser direcionadas ao Departamento de Tecnologia da Informação.

2.6. As caixas postais utilizadas por servidores que vierem a ser exonerados serão mantidas por 30 (trinta) dias, mediante configuração de direcionamento de mensagens para outras caixas postais, conforme indicação do departamento ao qual o servidor exonerado estiver vinculado. Após esse período, a caixa postal será excluída permanentemente. O direcionamento deverá ser solicitado do Departamento de Tecnologia da Informação, pelo respectivo superior hierárquico do servidor exonerado.

3. Utilização dos recursos do sistema de correio eletrônico

3.1. O uso do correio eletrônico do SEPREV é exclusivo para a execução da atividade institucional da Autarquia, sendo proibido seu uso para outros fins.

3.2. É de responsabilidade de cada colaborador o monitoramento frequente da sua caixa postal, bem como do espaço de armazenamento disponível.

3.3. O SEPREV poderá instituir mecanismos de monitoramento das mensagens enviadas e recebidas pelas contas de e-mail corporativas de todos os colaboradores.

3.4. É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

a) informações privilegiadas, confidenciais e/ou de propriedade do SEPREV para destinatários não autorizados;

b) materiais obscenos, ilegais ou antiéticos;

c) materiais preconceituosos ou discriminatórios;

d) materiais caluniosos ou difamatórios;

e) propaganda com objetivo comercial ou distinto dos objetivos da Autarquia;

f) listagem com endereços eletrônicos institucionais;

g) malwares;

h) material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;

i) material protegido por lei de propriedade intelectual;

j) entretenimentos e “correntes”;

l) assuntos ofensivos;

m) músicas, vídeos ou animações que não sejam de interesse específico do trabalho; e

n) Spam, phishing e hoax.

3.5. O acesso à caixa postal poderá ser feito via dispositivo móvel do próprio colaborador.

3.6. O uso do serviço de correio eletrônico deverá garantir que as mensagens estarão salvas na estrutura da empresa provedora do serviço (nuvem), não sendo permitido o uso de protocolos semelhantes ao POP - Post Office Protocol, que descarregam as mensagens no computador do usuário apagando-as do servidor da nuvem.

ANEXO II – PORTARIA Nº 437/2020
NCS-02 – SERVIÇO DE INTERNET
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Conceitos e Definições

1.1. Vírus: software malicioso que, como um vírus biológico, infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática com o objetivo de comprometer a integridade e a segurança.

1.2. Worm: é um programa autorreplicante, diferente de um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se alastrar, o worm é um programa completo e não precisa de outro para se propagar. Um worm pode ser projetado para tomar ações maliciosas após infestar um sistema.

1.3. Cavalo de troia: é um tipo de malware que, frequentemente, está disfarçado de software legítimo. Eles podem ser empregados por criminosos virtuais e hackers para tentar obter acesso aos sistemas dos usuários.

2. Utilização do serviço de Internet no SEPREV

2.1. Os equipamentos e serviços fornecidos para o acesso à internet são de propriedade do SEPREV, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privativas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

2.2. Qualquer informação acessada, transmitida, recebida ou produzida na internet, a partir da rede de computadores do SEPREV, está sujeita a divulgação e auditoria, tendo o SEPREV, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

2.3. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no SEPREV e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo respectivo superior hierárquico e homologados pelo Departamento de Tecnologia da Informação.

2.4. Os colaboradores não poderão utilizar os recursos do SEPREV para fazer o download ou distribuição de software ou dados não licenciados, conhecidos como “softwares piratas”.

2.5. É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

2.6. Os colaboradores não poderão utilizar os recursos do SEPREV para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

ANEXO III – PORTARIA Nº 437/2020
NCS-03 – COMPUTADORES, SOFTWARES E OUTROS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Conceitos e Definições

1.1. Computador: equipamento do tipo “mesa” (desktop) ou portátil (notebook).

1.2. Site: local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia. Exemplo: www.seprev.sp.gov.br

1.3. Proxy: serviço intermediário entre o usuário e a rede mundial de computadores (internet), onde podem ser aplicadas regras de negócio, como filtragem de conteúdo.

1.4. Firewall: é um dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede ou a toda uma rede de computadores.

2. Utilização dos computadores, softwares e outros recursos de tecnologia da informação no SEPREV

1. Os computadores disponibilizados aos colaboradores pelo SEPREV constituem instrumento de trabalho para execução das atividades institucionais.

2. Cada colaborador deve zelar para segurança e bom uso dos computadores e outros equipamentos fornecidos pelo SEPREV, reportando ao Departamento de T.I. qualquer incidente que tenha conhecimento e que possa comprometer a segurança ou a integridade dos equipamentos.

3. Em caso de mau uso, ou uso em desacordo com as instruções desta norma, o colaborador poderá ser responsabilizado, nos termos da Política de Segurança da Informação e do Estatuto dos Servidores Públicos Municipais de Indaiatuba.

4. Qualquer alteração dos parâmetros de segurança dos dispositivos, realizada por qualquer colaborador sem o devido credenciamento e a autorização para tal, poderá ser julgada inadequada e os riscos ou prejuízos causados relacionados serão informados ao colaborador e ao respectivo superior hierárquico, além da aplicação de penalidades vigentes.

5. O uso de qualquer recurso do SEPREV para atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Autarquia cooperará ativamente com as autoridades competentes.

7. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

8. Os computadores deverão ser instalados juntamente com nobreaks, evitando danos causados por oscilações na rede elétrica.

9. Deverá ser executada manutenção preventiva anual dos nobreaks e de outros mecanismos de proteção dos computadores e equipamentos de rede.

10. A rede de computadores do SEPREV disponibilizará diretórios compartilhados, com uso restrito a cada departamento (unidade P:\), e também diretórios com acesso exclusivo a cada usuário (unidade U:\).

10.1. Arquivos pessoais e outros não relacionados às atividades institucionais da Autarquia, não deverão ser armazenados nos diretórios da rede. Esse ambiente de armazenamento é exclusivo para arquivos de interesse do SEPREV.

10.2. Os colaboradores deverão armazenar os arquivos de interesse do SEPREV nos diretórios compartilhados de rede, os quais possuem mecanismos de segurança que garantem a integridade e a disponibilidade dos dados, bem como possuem rotinas automatizadas que realizam cópias de segurança dos arquivos.

10.3. Caberá ao departamento de TI fazer verificações periódicas no ambiente compartilhado de rede, a fim de identificar e eliminar arquivos que estejam em desacordo com as instruções desta Norma.

11. A rede de computadores do SEPREV deverá ser protegida com:

a) aplicativos contra vírus e outras pragas virtuais que possam comprometer a segurança ou a integridade dos dados;

b) solução de segurança tipo “firewall”, que implemente regras e instruções para garantir que somente a recepção ou envio de dados autorizados sejam trafegados pela rede; e

c) sistema de proteção para o acesso à internet (proxy), que implemente regras e instruções que impeçam o acesso a sites e recursos da internet que possam prejudicar a integridade ou a segurança da rede e dos dados armazenados.

11.1. A ausência de bloqueio de sites e serviços na internet pelos mecanismos de proteção estabelecidos pelo SEPREV não valida seu acesso, devendo ser observadas as restrições estabelecidas pela Política de Segurança da Informação e normas complementares.

ANEXO IV – PORTARIA Nº 437/2020
NCS-04 – IDENTIFICAÇÃO E CONTROLE DE ACESSO
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Conceitos e Definições

1.1. Recursos tecnológicos: qualquer equipamento de tecnologia disponibilizado pelo SEPREV aos seus colaboradores, para o exercício de suas atividades, como por exemplo computador, notebook, sistemas, etc.

1.2. Credencial de acesso: usuário e senha exclusivos que o SEPREV fornece a cada colaborador, para acesso aos recursos tecnológicos. São dados exclusivos e intransferíveis. Também podem ser fornecidos tokens de autenticação, cartões de CPF/CNPJ com assinaturas digitais, e outros dispositivos semelhantes que tem como objetivo autenticar o usuário.

2. Regras para identificação e controle de acesso no SEPREV

2.1. Para o acesso aos recursos tecnológicos do SEPREV será exigido, sempre que possível, identificação exclusiva de cada colaborador, permitindo assim o controle de acesso.

2.2. O compartilhamento de credenciais de acesso entre os colaboradores deve ser evitado sempre que possível.

2.3. Recomenda-se que o usuário seja direcionado a trocar imediatamente a sua senha ao realizar o primeiro acesso aos recursos de tecnologia.

2.4. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

2.5. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido às suas credenciais.

2.6. Os sistemas desenvolvidos ou contratados pelo SEPREV deverão manter trilhas de auditoria que permitam identificar, quando um dado for inserido ou alterado: qual usuário alterou, quando ocorreu a alteração, qual era a informação anterior e qual foi a informação nova registrada.

2.7. Os diretórios de rede implementados para permitir o compartilhamento de arquivos entre os colaboradores, deverão possuir mecanismos de segurança que garantam a confidencialidade e integridade dos dados, ou seja, somente os

usuários permitidos podem acessar e alterar os arquivos disponíveis nos diretórios compartilhados.

2.8. Os dados de acessão deverão ser suspensos temporariamente no caso de ausências superiores a 45 (quarenta e cinco) dias, e cancelados permanentemente no caso de exoneração do cargo ocupado no SEPREV.

2.8.1. Compete ao Departamento Administrativo comunicar, ao Departamento de TI, as ausências superiores a 30 (trinta) dias e as exonerações.

2.9. O acesso remoto aos sistemas do SEPREV, assim entendido como o acesso aos sistemas fora da rede de computadores disponível na sede do SEPREV, depende de autorização prévia do Departamento de TI.

2.9.1. Os colaboradores poderão acessar o ambiente do e-mail corporativo fora das dependências do SEPREV, mediante obtenção de instruções junto ao Departamento de TI.

2.10. O acesso ao ambiente de servidores e aos demais equipamentos da rede central de computadores do SEPREV, bem como aos servidores e serviços instalados em ambiente datacenter contratado pelo SEPREV, deve ser restrito à equipe de TI e, quando necessário, a prestadores de serviços e outros interessados, sempre devidamente acompanhados por colaborador da área de TI.

2.11. O acesso remoto aos serviços e sistemas instalados no ambiente local SEPREV ou em ambiente datacenter, por empresas contratadas, para execução de quaisquer serviços, deverá ser acompanhado por colaborador do Departamento de TI.

2.12. O acompanhamento de que trata o item anterior poderá ser dispensado, desde que:

a) O recurso tecnológico a ser acessado pela empresa seja de uso exclusivo de seus serviços fornecidos ao SEPREV, como por exemplo um servidor de aplicações ou um servidor de banco de dados. Desse modo, qualquer ação que possa comprometer o funcionamento dos serviços presentes nesse recurso tecnológico não prejudicará outros serviços que não são de responsabilidade dessa empresa; e

b) A empresa assine termo de responsabilidade quanto à segurança e a integridade dos dados, serviços e sistemas que terá acesso.

ANEXO V – PORTARIA Nº 437/2020
NCS05 - PROCEDIMENTOS DE CONTINGÊNCIA
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Conceitos e Definições

1.1. Procedimentos de contingência: ações a serem adotadas em caso de situações adversas, que causem perda de dados ou prejuízo ao funcionamento de recursos tecnológicos.

2. Dos procedimentos de contingência a serem adotados

2.1. Para garantir a segurança da informação, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo SEPREV, bem como dos arquivos de dados produzidos pelos colaboradores.

2.2. As rotinas de cópia de segurança deverão, sempre que possível, ser realizadas de forma automatizada, em horários pré-definidos, com armazenamento em local físico distinto de sua origem.

2.3. De acordo com critérios estabelecidos pelo departamento de Tecnologia da Informação, alguns dados poderão possuir cópias de segurança armazenadas no mesmo local físico do dado original, porém em dispositivo de armazenamento distinto.

2.4. Deverá ser executada periodicamente a verificação da integridade das cópias de segurança dos arquivos de dados, sistemas de informação e respectivos bancos de dados.

2.5. Tabela de dados que devem ser realizadas cópias de segurança:

DADOS DO SEPREV E RESPECTIVOS PROCEDIMENTOS DE BACKUP

Tipo de dado	Periodicidade do backup	Local de armazenamento	Tempo de armazenamento	Observações
Arquivos salvos dos diretórios compartilhados de rede (unidades P:\ e U:\)	Mensalmente dia 15	HD Externo/Storage	Somente a última cópia	A estrutura atual de armazenamento contempla redundância de disco rígido (RAID 1), ou seja, os arquivos são salvos em 2 HDs em modo "espelhamento" – sincronização em tempo real.
Arquivos salvos nos computadores dos usuários/colaboradores	Não aplicável	Não aplicável	Não aplicável	O usuário deve salvar arquivos de interesse do SEPREV nos diretórios compartilhados da rede (unidades P:\ ou U:\)
CECAM – Banco de dados (ano atual e ano anterior)	Diariamente às 19h	SEPREV-WIN01	1 dia	Manual 004 - TI
	Último sábado de cada mês	SERVER02	1 dia	
	Dia 1 de cada mês	Nuvem corporativa	5 anos	
CECAM – Aplicação	Dia 1 de cada mês	SERVER02	Somente a última cópia	
Bancos de dados SQL Server01	Toda sexta às 20:30h	SEPREV-WIN01	1 semana	Arrecadação,

	Último sábado de cada mês, às 10h	SERVER02		SIMPS (seprev), ASPPREV, INTEGRAÇÃO Manual 003 - TI
	Dia 1 de cada mês	Nuvem corporativa	5 anos	
Banco de dados SISPREV (previdência)	Diário às 18h	SEPREV-WIN01	5 dias	
	Última sexta-feira do mês	SERVER02	Somente a última cópia	
	Dia 1 de cada mês	Nuvem corporativa	5 anos	
Aplicação SISPREV (previdência)	Dia 1 de cada mês	SERVER02	Somente a última cópia	
Banco de dados FACPLAN (Saúde)	Dia 1 de cada mês	HD Externo/Storage e/ou nuvem corporativa	Somente a última cópia	O banco de dados está instalado em ambiente nuvem (Amazon) de responsabilidade da empresa fornecedora. São realizados backups diários da base de dados, sendo que a cada 15 minutos o ambiente é replicado, a fim de garantir continuidade em caso de incidente. A equipe de TI tem acesso aos backups.
Aplicação FACPLAN (Saúde)	Não necessário	Não necessário	Não necessário	O sistema está instalado em ambiente nuvem (Amazon) da empresa fornecedora, com

				replicação para garantir continuidade. O SEPREV possui instalação local da aplicação.
Aplicativo Boletos – Caixa	Diário às 20:30h, realizado no Cobian do SERVER02	SERVER02	Somente a última cópia	
Aplicativo – Start PABX	Toda sexta-feira às 19:00h, realizado no Cobian do SERVER02	SERVER02	Somente a última cópia	Armazena o histórico de ligações efetuadas e recebidas – 38254600 e seus ramais
	Dia 1 de cada mês	Nuvem corporativa	5 anos	
Site – fazer uma cópia *full* da máquina virtual	Não necessário	Não necessário	Não necessário	Ambiente já possui backups efetuados pelo datacenter (Equinix), previsto em contrato
Site – cópia da estrutura do site	Não necessário	Não necessário	Não necessário	Ambiente já possui backups efetuados pelo datacenter (Equinix), previsto em contrato Além disso, equipe de TI possui ambiente local com cópia idêntica do site (com controle de versões)

Bancos de dados MYSQL – site	Toda sexta-feira, às 20h	SERVER02	Somente a última cópia	Ambiente já possui backups efetuados pelo datacenter (Equinix), previsto em contrato. Equipe de TI do SEPREV faz backup semanal para ambiente de homologação
Backup do Estado do Sistema – Servidor Local	Mensalmente no dia 15	HD Externo/Storage	Somente a última cópia	A estrutura atual de armazenamento contempla redundância de disco rígido (RAID 1), ou seja, os arquivos são salvos em 2 HDs em modo "espelhamento" – sincronização em tempo real.
Dispositivos de gravação de imagens (DVR) – câmeras internas	Mensalmente no dia 15	HD Externo/Storage	Somente a última cópia	Armazenamento atual mantém aproximadamente 45 dias de histórico
Dispositivos de gravação de imagens (DVR) – câmeras externas	Mensalmente no dia 15	HD Externo/Storage	Somente a última cópia	Armazenamento atual mantém aproximadamente 100 dias de histórico
Servidor virtual SERVER01	Mensalmente no dia 15	HD Externo/Storage	6 meses	A estrutura atual de armazenamento

				contempla redundância de disco rígido (RAID 1), ou seja, os arquivos são salvos em 2 HDs em modo “espelhamento” – sincronização em tempo real.
Servidor virtual SERVER02	Mensalmente no dia 15	HD Externo/Storage	6 meses	A estrutura atual de armazenamento contempla redundância de disco rígido (RAID 1), ou seja, os arquivos são salvos em 2 HDs em modo “espelhamento” – sincronização em tempo real.

Definições:

- SERVER01 – servidor instalado no ambiente local do SEPREV
- SERVER02 – servidor instalado no ambiente local do SEPREV
- SEPREV-WIN01 – servidor instalado no datacenter contratado pelo SEPREV
- Nuvem corporativa – espaço de armazenamento contratado pelo SEPREV junto à Microsoft. O serviço é integrado com a conta de e-mail do Diretor do Departamento de TI.
- HD Externo/Storage: disco externo USB.

ANEXO VI – PORTARIA Nº 437/2020
NCS-06 – Orientações específicas para os colaboradores do Departamento de Tecnologia da Informação
(Norma Complementar de Segurança - Política de Segurança da Informação)

1. Orientações específicas para os colaboradores que atuam no Departamento de Tecnologia da Informação

1.1. Manter sigilo sobre os dados e informações que tiver acesso, não as utilizando, em hipótese nenhuma, para fins que não sejam de interesse do SEPREV.

1.2. Não usar as informações que tiver acesso para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros.

1.3. É proibido efetuar cópias de documentos e arquivos dos computadores e servidores da infraestrutura do SEPREV, salvo se solicitado pela direção ou aqueles contemplados por rotinas de backup estabelecidas.

1.4. Não apropriar, para si ou para outrem, de material confidencial e/ou sigiloso que, por motivo de atuar no departamento de TI venha a ser acessível ou disponibilizado.

1.5. Zelar pela segurança de seus dados de acesso a recursos e sistemas (logins e senhas), **especialmente os acessos do tipo "Administrador",** devendo os mesmos serem armazenados de forma segura, responsabilizando-se pela má guarda, má utilização e eventuais consequências.

1.6. Atuar pró-ativamente na correção ou ajuste de vulnerabilidades ou condutas de usuários, que venha a ter conhecimento, caso estas possam prejudicar a segurança da informação no SEPREV.

1.7. Na manutenção de dados nos sistemas gerenciadores de banco de dados, deve-se SEMPRE utilizar procedimentos que permitam rollback de transações.

1.8. Configurar os equipamentos e sistemas de modo a atender as diretrizes da Política de Segurança e de suas respectivas Normas Complementares de Segurança.

1.9. Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.

1.10. Realizar inspeções periódicas de configurações técnicas e análise de riscos.

1.11. Propor sistemas e processos específicos que visem aumentar a segurança da informação.

1.12. Promover a conscientização dos colaboradores, dos segurados e dos beneficiários em relação à relevância da segurança da informação.