FUNDO DE PREVIDÊNCIA DO RPPS DE VIÇOSA DO CEARÁ - VIÇOSAPREV

Portaria nº 028/2015

DISPÕE SOBRE OS ESCLARECIMENTOS DA POLITICA DE SEGURANÇA DAS INFORMAÇÕES- PSI E AS ADEQUAÇÕES DA PSI DO VIÇOSA-PREV

A Diretoria-Executiva do Fundo de Previdência do RPPS do município de Viçosa do Ceará/CE – VIÇOSA-PREV, no uso de suas atribuições legais, conferidas pelos §§ 1º e 2º do Art. 12 da Lei 489/2007- Decreto 209/2015, de 02 de dezembro de 2015 C/C com o Art. 81 da Lei Orgânica do Município;

CONSIDERANDO QUE A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais.

CONSIDERANDO QUE a politica de segurança deve iniciar com o fortalecimento da cultura de proteção a informações;

CONSIDERANDO QUE O VIÇOSAPREV armazena informações cadastrais, funcionais e financeiras dos servidores segurados obrigatórios do RPPS de Viçosa do Ceará-CE

CAPÍTULO I
DOS FUNDAMENTOS

Art 1º - Um sistema de segurança da informação baseia-se em três princípios básicos:

a)confidencialidade,

b) integridade e

c)disponibilidade.”

§ 1º Se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que venha a comprometer qualquer um desses princípios, atentará contra a sua segurança.

§2º Confidencialidade : A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso . Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física.

§3º Integridade : A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento .Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente. Quando a informação é alterada, falsificada ou furtada, ocorre à quebra da integridade. A integridade é garantida quando se mantém a informação no seu formato original.

§ 4º Disponibilidade : A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário . Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes por conta de ataques e invasões, considera-se um incidente de segurança da informação por quebra de disponibilidade. Mesmo as interrupções involuntárias de sistemas, ou seja, não intencionais, configuram quebra de disponibilidade.

Art. 2º Sobre o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO deve-se obedecer as seguintes normas de Política de segurança da informação;

a)organização da segurança da informação;
b)gestão de ativos;
c)segurança em recursos humanos;
d)segurança física e do ambiente;

e)gestão das operações e comunicações;
f)controle de acesso;
g)aquisição, desenvolvimento e manutenção de sistemas de informação;
h)gestão de incidentes de segurança da informação;
i)gestão da continuidade do negócio, e conformidade.

Paragrafo Único - O sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

Art 3º - CLASSIFICANDO AS INFORMAÇÕES

a) A principal razão em classificar as informações, é de que elas não possuem o mesmo grau de confidencialidade, ou então as pessoas podem ter interpretações diferentes sobre o nível de confidencialidade da informação.

b) Antes de se iniciar o processo de classificação, é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações.

c) As informações podem ser classificadas em informações públicas, quando não necessita de sigilo algum; informações internas, quando o acesso externo as informações deve, ser negado; e informações confidenciais, as informações devem ser confidenciais dentro da empresa e protegida contra tentativas de acesso externo.

Art. 4º - A definição clássica é que o ativo compreende ao conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa .

Paragrafo único - A informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo.

Art. 5º - A ameaça pode ser considerada um agente externo ao ativo de

informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação – a confidencialidade, integridade ou disponibilidade.

Paragrafo Único - As ameaças podem ser, naturais: são aquelas que se originam de fenômenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano, e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como hacker.

Art. 6º - A vulnerabilidade é definida como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação.

§ 1º - Ao terem sido identificadas as vulnerabilidades ou os pontos fracos, será possível dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

§2º As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegida contra incêndios, inundações, e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e insatisfatório nos locais de trabalho; ausência de procedimento de controle de acesso e utilização de equipamentos por pessoal contratado; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; software sem patch de atualização e sem licença de funcionamento.

Art. 7º Com relação a segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Art. 8º - Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar a empresa a problemas graves, é necessário a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois especificado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminar os riscos a que o órgão se encontra sujeita.

Art. 9º - O backup dos sistemas deve ser armazenado em outro local, o mais longe possível do ambiente atual, como em outro prédio. O procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro.

Art. 10 - Convém que sejam utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação.

Art. 11 - Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzirá resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em todo o órgão e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita a própria área e somente durante a execução das atividades em que ela se torna necessária.

Paragrafo Único - Os locais escolhidos para a instalação dos equipamentos devem estar em boas condições de uso, com boas instalações elétricas, saídas de emergência, alarme contra incêndio, devem conter extintores de incêndios, entre outros aspectos que devem ser levados em consideração.

CAPÍTULO II
DOS ATOS NORMATIVOS

Art. 12 – A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI pode-se definir como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

§ 1º Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras pré-estabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir.

§2º A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por, exemplo a indisponibilidade do serviço, furto ou até

mesmo a perda de informações.

§3º As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pele experiência do gestor.

§4º O intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porém, deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização.

§5º É recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

Art. 13 A política de segurança da informação deve estabelecer:

§ 1º Como será efetuado o acesso as informações de todas as formas possíveis, seja ela internamente ou externamente;

§ 2º Quais os tipos de mídias poderão transportar e ter acesso a esta informação.

§ 3º A política deve especificar os mecanismos através dos quais estes requisitos podem ser alocados.

CAPÍTULO III
DA ORGANIZAÇÃO E DO CUMPRIMENTO

Art. 14 A política de segurança da informação do VIÇOSA-PREV comporá de um gestor de área afins do município que tenha responsabilidade de gestão.

§ 1º - – A responsabilidade das informações do VIÇOSA-PREV está com a Secretaria de Logística e Estrategia administrativa – SELOG , devido esta Unidade Gestora ainda ser vinculada a administração direta, ressaltando que as informações são armazenadas em servidores de redes exclusivo do VIÇOSA-PREV.

§ 2º – Os servidores de redes do VIÇOSAPREV encontram -se na sede do NTI- SELOG , tanto o adquirido com recursos próprios e o recebido

pelo PROPREV 2 para condicionamento das informações exclusivas do VIÇOSAPREV.

§3 º No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade.

§4º O conjunto de normas e regras que regulem a utilização dos sistemas das empresas, assim como o acesso a redes sociais e e-mails pessoais.

§5º Também é importante lembrar que os servidores devem estar cientes do monitoramento.

Art. 15 A política de segurança da informação do VIÇOSA-PREV estende também a empresa terceirizada onde mantêm o site www.vicosaprev.com.br , os serviços on line e os e-mail institucionais, onde tem regras específicas, porém que atendem a politica de segurança de informação da contratada.

Art. 16 Quando necessário será contratada empresa especializada para estudo das vulnerabilidades e se existir será realizado ações para saná-las.

Art. 17 Quando da necessidade de cadastramento de um novo usuário para utilização do SIPREV , ou outros sistemas ou equipamentos de informática o VIÇOSA-PREV - setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

Art. 18 É terminantemente proibido o uso de programas ilegais (PIRATAS) . Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos . Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Art. 19 O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva

do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

Art. 20 O setor de de Pessoal deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema do Órgão. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Art. 21 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 funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do VIÇOSA-PREV.

Art. 22- É de propriedade do VIÇOSA-PREV, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício.

CAPÍTULO IV
DO ACESSO E DAS PROIBIÇÕES

Art. 23 O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais . Sites que não contenham informações que agreguem conhecimento profissional e/ou para o desenvolvimento do trabalho não devem ser acessados.

§ 1º O uso da Internet será monitorado pelo Setor de Informática, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

§ 2º A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da diretoria do VIÇOSA-PREV com base em recomendação do Setor de Informática.

§ 3º Não é permitido instalar programas provenientes da Internet nos

microcomputadores do órgão , sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

§ 4º Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

§ 5º Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

a)De estações de rádio;
b)De conteúdo pornográfico ou relacionados a sexo;
c)Que defendam atividades ilegais;
d) Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
e) Que promovam a participação em salas de discussão de assuntos não relacionados aos serviços;
f)Que promovam discussão pública sobre os assuntos do órgão, a menos que autorizado pela Diretoria;
g) Que possibilitem a distribuição de informações de nível "Confidencial".
h) Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Art. 24 O correio eletrônico fornecido pelo VIÇOSAPREV é um instrumento de comunicação interna e externa para a realização do negócio Órgão.

§ 1º As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem VIÇOSAPREV , não podem ser contrárias à legislação vigente e nem aos princípios éticos do VIÇOSAPREV.
§ 2º O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Art. 25 É terminantemente proibido o envio de mensagens que:

a) Contenham declarações difamatórias e linguagem ofensiva;
b)Possam trazer prejuízos a outras pessoas;

c) Sejam hostis e inúteis;
d) Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
e) Possam prejudicar a imagem da organização;
f) Possam prejudicar a imagem de outras empresas;
g))Sejam incoerentes com as políticas do VIÇOSAPREV.

§ 1º Para incluir um novo usuário no correio eletrônico, a Diretoria deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

§2º 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 mesmo.

Art. 26 O Setor de Informática é responsável pela aplicação da Política do órgão em relação a compra e substituição de "software" e "hardware".

Paragrafo Único - Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Art. 27 Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do VIÇOSA-PREV , devem estar cientes de que:

§ 1º Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo realização de atividades profissionais.
§ 2º A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
§ 3º É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
§ 4º O usuário não deve alterar a configuração do equipamento recebido.

Art. 28 Alguns cuidados que devem ser observados:

§ 1º Fora do trabalho:

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

§ 2º Em caso de furto

a)Registre a ocorrência em uma delegacia de polícia;
b)Comunique ao seu superior imediato e ao Setor de Informática;
c) Envie uma cópia da ocorrência para o Setor de Informática.

Art. 29 Os responsáveis pelos setores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações , cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

Paragrafo Unico - O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

a)Que tipo de informação o usuário pode acessar;
b)Quem está autorizado a acessar determinada rotina e/ou informação;
c)Quem acessou determinada rotina e informação;
d)Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
e)Que informação ou rotina determinado usuário acessou;
f)Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

Art. 30 Todo arquivo em mídia proveniente de entidade externa a o órgão deve ser verificado por programa antivírus.

§ 1º Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

§2º Todas as estações de trabalho devem ter um antivírus instalado. A

atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

§ 3º O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

CAPÍTULO V
DO CUMPRIMENTO DAS ORIENTAÇÕES

Art. 31 – O não cumprimento da Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, e exoneração do cargo.

§ 1º - Respeitar-se-á a Lei 485/2007 – Estatuto dos Servidores Públicos no que se refere ao Regime Disciplinar.

§2º - No que couber, outra ação disciplinar e/ou processo civil ou criminal dependendo da gravidade.

Viçosa do Ceará, 28 de dezembro de 2015

MARIA DAS GRAÇAS ALVES SILVA
Diretora-Excutiva do VIÇOSA-PREV