POLITICA DE SEGURANÇA DA INFORMAÇÃO

Instituto de Previdência dos Servidores Públicos Municipais de Cascavel – CAPREV
11.598.569/0001-17 – e-mail: cascavelcaprev@gmail.com

Art. 1º. **DISPOR e DAR** conhecimento a todos os servidores do Instituto de Previdência dos Servidores Públicos Municipais de Cascavel – CAPREV acerca das regras que se seguem que compõe a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI.**

DOS FUNDAMENTOS

Art. 2º. Um sistema de segurança da informação baseia-se em três princípios básicos:

a) Confidencialidade;
b) Integridade;
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 não permitir que a informação 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 ainformação 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. 3º Sobre o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) devem-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;
j) Sigilo sobre as informações acessadas pelos integrantes do CAPREV.

Parágrafo 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. 4º. As informações podem ser classificadas em:

a) informações públicas, quando não necessita de sigilo algum;
b) informações internas, quando o acesso externo as informações deve, ser negado;
c) informações confidenciais, quando essas devem ser confidenciais tanto dentro da empresa quanto fora dela e protegidas contra tentativas de acesso interno e/ou externo.

§ 1º – 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;

§ 2º – 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.

Art. 5º. 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.

Parágrafo 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. 6º. A ameaça pode ser considerada um agente externo ao ativo de informação,pois se aproveita de suas vulnerabilidades para quebrar um ou mais dos princípios básicos da segurança da informação – a confidencialidade, integridade e/oudisponibilidade.

Parágrafo único – As ameaças podem ser divididas nos seguintes tipos básicos:
a) As naturais – são aquelas que se originam de fenômenos da natureza;
b) As involuntárias – são as que resultam de ações desprovidas de intenção para causar algum dano,
c) As intencionais – são aquelas deliberadas, que objetivam causar danos, tais como às realizadas pelos hackers ou crackers.

Art. 7º. 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 asfraquezas 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 Após terem sido identificadas as vulnerabilidades ou os pontos fracos, é possível dimensionar os riscos ao qual o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

§ 2º As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegidas contra incêndios, inundações, desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e/ou locais de trabalho insatisfatórios; ausência ou não utilização de procedimento de controle de acesso e/ou utilização de equipamentos por pessoal contratado sem a observância dos requisitos citados anteriormente ou desautorizados; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; além de softwares sem patch de atualização e/ou sem licença de funcionamento.

Art. 8º Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam os potenciais de danos e perdas, sendo medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Art. 9º Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar o ente a problemas graves, é necessária a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois realizado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminá-los a que o órgão possa estar sujeito além de garantir melhor eficiência nas ações preventivas.

Art. 10 O backup dos sistemas deve ser armazenado periodicamente em outra mídia, e guardado o mais longe possível do ambiente atual, como em outro setor (cofre da instituição, por exemplo). O procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação por conta da ocorrência de algum sinistro.

Art. 11 Convém que sejam utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação.

Art. 12 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 todoo 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.

Parágrafo único Os locais escolhidos para a instalação dos equipamentos devem estar em boas condições de uso, com boas instalações elétricas, entre outros aspectos que devem ser levados em consideração.

DOS ATOS NORMATIVOS

Art. 13 A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI pode ser definida como um documento que estabelece princípios, valores, compromissos, requisitos, orientações eresponsabilidades 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 recursosde TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras preestabelecidas, 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 pela 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.

§6º A política de segurança não define só procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas e funcionários) que lidam com essa informação.

Art. 14 A política de segurança da informação deve estabelecer:

a) Como será efetuado o acesso às informações de todas as formas possíveis, seja ela internamente ou externamente;
b) Quais os tipos de mídias poderão transportar e ter acesso a esta informação;
c) Os mecanismos através dos quais estes requisitos podem ser alocados.

DA ORGANIZAÇÃO E DO CUMPRIMENTO

Art. 15 A política de segurança da informação do CAPREV comporá de um gestor de área afins da Unidade Gestora que tenha responsabilidade de gestão.

§ 1º A responsabilidade das informações do CAPREV está sob a responsabilidade da proteção dos dados é dos Dirigentes, ressaltando que as informações deverão serem armazenadas em servidores de redes exclusivos do CAPREV.

§ 2º Os servidores de redes do CAPREV atualmente são feitos por computadores/desktops que executam essa função e deverão encontrar-se na sede do instituto para condicionamento das informações exclusivas do mesmo.

§3º Deverão ser digitalizados todos os processos, com o devido armazenamento em Drive na nuvem e a manutenção de backups nos computadores do instituto.

§ 4º No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação - TI, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade.

§ 5º 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.

§ 6º Os servidores deverão estar cientes do monitoramento.

Art. 16 A política de segurança da informação do CAPREV estende também à empresa terceirizada onde mantêm o site https://caprevcascavel.com.br, serviços on-line, aplicativos administrativos e os e-mails institucionais, onde tem regras específicas, porém que atendem a política de segurança de informação da contratada.

Art. 17 Quando necessário será contratada empresa especializada para estudo das vulnerabilidades e se existir será realizado ações para saná-las.

Art. 18 Quando da necessidade de cadastramento de um novo usuário para utilização de sistemas ou equipamentos de informática no CAPREV, o setor de origem do novo usuário deverá comunicar esta necessidade aos Diregentes por meio de memorando, e-mail ou correio interno, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

Art. 19 É terminantemente proibido o uso de programas ilegais (PIRATAS) e/ou desautorizados pela UG Previdenciária. Os usuários não podem, em hipótese alguma, instalar este tipo de “software” (programa) nos equipamentos/computadores e afins. Periodicamente, o Setor de Informática (TI) fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Art. 20 O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva dos Dirigentes, assim como a manutenção, alteração e atualização de equipamentos e programas.

Art. 21 Os Dirigentes deverão informar ao administrador do site/sistemas, 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 Responsável.

Art. 22 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 IPSGA.

Art. 23 É de propriedade do CAPREV, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício.

DO ACESSO E DAS PROIBIÇÕES

Art. 24 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 a luz das normas vigentes, 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 Interneté atribuição da unidade gestora do CAPREV ou responsável definido pela mesma, com base, também, em recomendação.

§ 3º Não é permitido instalar programas provenientes da Internet nos microcomputadores do órgão, sem expressa anuência, exceto os programas oferecidospor órgãos públicos federais, estaduais e/ou municipais, todos previamente informadosaos Dirigentes.

§ 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/uploads), cópia ou qualquer outro tipo de acesso a sites:

a) De estações de rádio;

b) De conteúdos pornográficos 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 autorizadopela Diretoria;

g) Que possibilitem a distribuição de informações de níveis “Confidenciais”;

h) Que permitam a transferência (downloads ou uploads) de arquivos e/ou programas ilegais;

i) Que permitem a transferência (downloads ou uploads) de arquivos e/ou programas que promovam o acesso remoto a qualquer dispositivo do CAPREV, sem a anuência do Setor Responsável;

j) Que permitam a transferência (downloads ou uploads) de arquivos e/ou programas que busquem na rede interna e/ou externa vulnerabilidades em dispositivos e/ou serviços de qualquer natureza, salvo em casos de anuência da gestora e/ou Setor de Informática (TI);

k) Que permitam o uso e/ou armazenamento de programas e/ou serviços relacionadosa entretenimento tais como jogos, karaokê e desafios (ou similares);

§ 6º Será disponibilizado um servidor de arquivos, contendo diretórios para cada setor do CAPREV onde os funcionários lotados no setor específico terão acesso, e ainda será disponibilizado acesso comum a setores distintos e/ou a todos os setores quando os dados constantes nos diretórios subsidiar o desenvolvimento do trabalho da Instituiçãoem mais de um setor, assim será cognominado o diretório de “PublicoNet”.

§ 7º A Diretoria do CAPREV na pessoa do gestor terá acesso a todos os diretórios da Instituição.

Art. 25 O correio eletrônico fornecido pelo CAPREV é um instrumento de comunicação interna e externa para a realização do negócio do Órgão.

§ 1º As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do CAPREV, não podem ser contrárias à legislação vigente e nem aos princípios éticos do CAPREV.

§ 2º O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

§ 3º 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.

§ 4º 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 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 inúteis, 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 CAPREV.

Art. 27 O Setor de Informática é responsável pela aplicação da Política do órgão em relação à compra e substituição de "software" e "hardware".

Parágrafo 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. 28 Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do CAPREV, devem estar cientes de que:
a) Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo realização de atividades profissionais.
b) A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
c) É de responsabilidade de cada usuário assegurar a integridade do equipamento, aconfidencialidade e disponibilidade da informação contida no mesmo.
d) O usuário não deve alterar a configuração do equipamento recebido.

Art. 29 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, 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. 30 Os responsáveis pelos setores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações, cabendo a eles verificaremse 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.

§1º O Setor verificará se houve 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 determinada rotina ou informação;
e) Que informação ou rotina determinado usuário acessou;
f) Quem tentou acessar qualquer rotina ou informação sem estar autorizado.
g) Se algum usuário teve acesso de forma indevida a senhas de sistemas do CADPREV, BANCOS, E-MAIL e/ou tipos de sistemas.

§2º O exercício fiscalizatório acima previsto deverá ser exercido com moderação e estrita observância da necessidade de forma a não implicar em violação de intimidade de qualquer servidor ou de seus dados eletrônicos por parte do servidor, implicara em cometimento de crime previsto em Lei sobre a matéria.

§3º Todas as informações e dados colhidos no âmbito do CAPREV, no exercício do poder fiscalizatório enumerado no parágrafo 1º, é integralmente sigilosa, não podendo ser exposta a terceiro, devendo constar unicamente em relatório técnico que deve ser entregue diretamente à Gestão do CAPREV, para adoção das medidas cabíveis.

§4º Todos os funcionários que tenham acesso às informações de qualquer natureza, seja de processos eletrônicos ou físicos, dados eletrônicos e pessoais de segurados e funcionários do CAPREV, encontra-se vinculado a dever de sigilo profissional art. 154 do Código Penal e abrangido por obrigação civil de não fazer, sujeitando-se às penalidades previstas no art. 251 do Código Civil.

§5º Todos os dados que o setor de Tecnologia da Informação armazenar em dispositivos como pendrive, HD externo ou similar, por motivo de transferência de dados das máquinas, entre outros, deverão ser posteriormente excluídos de tais dispositivos com total segurança.

§6º Deverá o setor de TI ter uma rotina de verificação de máquinas e equipamentos de informática nos setores, recebendo a demanda dos usuários e realizando o atendimento.

Art. 31 Todo arquivo em mídia proveniente de entidade externa ao 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.

Art. 32 Quanto aos equipamentos e informações contidas nos mesmos:

a) É proibida a execução de programas externos nos computadores e/ou equipamentos do CAPREV sem o devido consentimento da gestora e/ou setor de informática;
b) É proibido abrir quaisquer equipamentos relacionados à área de informática (ou similares) com o intuito de realizar reparos, troca de peças, instalação de novos dispositivos ou complementos (físicos e/ou virtuais), sem o devido consentimento da gestora e/ou setor de informática;

c) Tornar ciente de que o CAPREV não é responsável por informações pessoais que não se referem à natureza de sua operação, definindo essas informações como sendo indevidas para uso interno à instituição;
d) É terminantemente proibido disseminar, intencional ou não, vírus ou qualquer programa que gere ameaça à continuidade do serviço.
e) É proibido o compartilhamento de senhas e/ou similares, sendo o usuário responsabilizado pelo seu uso indevido.

Art. 33 É proibido o uso de notebook ou similares, de propriedade privada dos funcionários do CAPREV, para uso no desenvolvimento de trabalhos da instituição e também de arquivamento de dados, sejam imagens, textos ou quaisquer dados exclusivo da Instituição.

Art. 34 Quando empresa contratada para prestação de serviços no CAPREV solicitar arquivos, banco de dados ou similares, o setor de TI só fornecerá mediante autorização do gestor.

DO CUMPRIMENTO DAS ORIENTAÇÕES

Art. 35 O não cumprimento da Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações:
a) advertência formal;
b) suspensão;
c) exoneração do cargo.

§ 1º Respeitar-se-á o Estatuto dos Servidores Públicos de Cascavel-CE no que se refere ao Regime Disciplinar ou outra Lei especifica que a determine.

§ 2º No que couber, outra ação disciplinar e/ou processo civil ou criminal poderá ser aplicado, a depender da gravidade da conduta.