POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Institui a Política de Segurança da Informação - PSI do INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS MUNICIPAIS DE UBERABA - IPSERV, e dá outras providências.

1. INTRODUÇÃO

A Política de Segurança da Informação, ou simplesmente "PSI" é um documento que orienta e estabelece as diretrizes corporativas do IPSERV – Instituto de Previdência dos Servidores Públicos Municipais de Uberaba para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27005:2008, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A informação é um ativo de grande valor para a IPSERV, por isso, necessita ser adequadamente protegida.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores, fornecedores e prestadores de serviços do IPSERV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da instituição e do indivíduo.

Garantir que os recursos computacionais e serviços de Tecnologia da Informação - TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar o IPSERV, colaboradores e terceiros.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Deve implementar controles para preservar os interesses do IPSERV contra danos que possam ser consideradas como violação ao uso dos serviços e, portanto, considerados vedados.

Preservar as informações do IPSERV quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Caso os procedimentos ou normas aqui estabelecidos sejam violados por usuários, a CODIUB informará aos órgãos competentes de forma que sejam tomadas medidas cabíveis.

3. APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores, bem como os fornecedores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada servidor, fornecedor e prestador de serviços de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo IPSERV pertence à referida instituição.

As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido dentro dos limites cabíveis, desde que não prejudique o desempenho dos sistemas e serviços.

O IPSERV, por meio de sua equipe de tecnologia de informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DAS RESPONSABILIDADES ESPECÍFICAS

DOS SERVIDORES E FORNECEDORES EM GERAL

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público ou cargo comissionado que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada servidor ou fornecedor todo prejuízo ou dano que vier a sofrer ou causar ao IPSERV e/ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.

DOS SERVIDORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS E ESTAGIÁRIOS):

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política de Segurança de Informações - PSI.

A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas nesta política.

DOS GESTORES DE PESSOAS E/OU PROCESSOS:

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.

Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação.

Exigir dos servidores a assinatura do Termo de Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPSERV.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

DA EQUIPE DE TECNOLOGIA DA INFORMAÇÃO:

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança de Informações.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o IPSERV.

Quando ocorrer movimentação interna dos ativos de tecnologia de informação, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Realizar auditorias periódicas de configurações técnicas e análise de riscos. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de exoneração de servidor, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do IPSERV.

Promover a conscientização dos servidores em relação à relevância da segurança da informação para as atividades precípuas ao IPSERV.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança da Informação - PSI, o IPSERV poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação dos Diretores;

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CONTROLE DO USO DE E-MAIL:

O objetivo é informar aos servidores do IPSERV quais são as atividades permitidas e vedadas quanto ao uso do e-mail corporativo.

A responsabilidade pela utilização do e-mail do IPSERV recai a todos os seus membros que efetivamente o utilizam, de modo que a averiguação de responsabilidade entre seus membros seja objetiva.

O uso do e-mail do IPSERV é para fins corporativos e relacionados às atividades da instituição.

A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o IPSERV e também não cause impacto no tráfego da rede.

É vedado aos servidores o uso do e-mail do IPSERV para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- enviar mensagem por e-mail pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPSERV ou suas unidades vulneráveis a ações civis ou criminais;

- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários com o objetivo de evitar as punições previstas;

- apagar mensagens pertinentes de correio eletrônico quando o IPSERV estiver sujeito a algum tipo de investigação;

- Utilizar o endereço de correio eletrônico corporativo para fins de cadastros pessoais e redes sociais;

- produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPSERV;

    - contenha ameaças eletrônicas, como: spam, mail *bombing*, vírus de computador etc.;

    - contenha arquivos com código executável (exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

    - vise obter acesso não autorizado a outro computador, servidor ou rede;

    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

    - vise burlar qualquer sistema de segurança;

    - vise vigiar secretamente ou assediar outro usuário;

    - vise acessar informações confidenciais sem explícita autorização do proprietário;

    - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

    - inclua imagens criptografadas ou de qualquer forma mascaradas;

- contenha anexo(s) superior(es) a 25 MB para envio (interno e internet) e 25 MB para recebimento (internet), exceto com autorização prévia do gestor da área;

- tenha conteúdo considerado impróprio, obsceno ou ilegal;

- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

- tenha fins políticos locais ou do país (propaganda política);

- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

CONTROLE DO USO DE INTERNET:

Todas as regras atuais do IPSERV visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o IPSERV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, 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 privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O IPSERV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os servidores que estão devidamente autorizados a falar em nome do IPSERV para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É vedada a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades no IPSERV e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

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 vedados. Qualquer software não autorizado baixado será excluído pela área de tecnologia de informação.

Os servidores não poderão em hipótese alguma utilizar os recursos do IPSERV para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Servidores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao IPSERV ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

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

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (SKYPE, WHATSAPP, redes sociais e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor ou a área de tecnologia da informação julgue necessário.

Não é permitido acesso a sites de proxy.

CONTROLE DE ACESSO À INFORMAÇÃO SENSÍVEL DE MEIO FÍSICO:

O objetivo é prevenir o acesso não autorizado as informações sensíveis de meio físico de posse e competência do IPSERV, evitando danos e interferências.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controlados e restrito às pessoas autorizadas. O acesso não autorizado não será permitido.

O controle de retirada e/ ou consulta das informações será controlado por responsável designado que fará monitoramento por meio de emissão de protocolos. As informações contidas no protocolo contam com no mínimo:

- nome e visto do servidor responsável emissor do protocolo;

- nome e visto do servidor interessado ao acesso da informação sensível de meio físico;
- a data e hora da retirada e/ou consulta da informação sensível de meio físico;
- a data e hora da devolução da informação sensível de meio físico e
- Observações Complementares.

A retirada de informações sensíveis de meio físico sem a devida emissão do protocolo não será autorizada.

Toda a informação sensível de meio físico será conferida no ato da devolução, estando sujeito a emissão de ocorrências em caso de desorganização, desleixo ou ausência de documentos.

São considerados os casos de desorganização e desleixo:

- Desordem na numeração das folhas do processo;
- Rasuras, anotações e amassados;
- Sujeiras de alimentos e bebidas.

Não é permitido a retirada de qualquer folha objeto de complemento ao arquivo de informação.

A possibilidade de foto cópia será permitida somente com a emissão do protocolo, onde deverá ser preenchido no item “Observações Complementares” as folhas que foram objeto da foto cópia.

Não é permitida a locomoção de informações sensíveis de meio físico fora as dependências do IPSERV, sem prévia autorização.

6. IDENTIFICAÇÃO:

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o IPSERV e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados no IPSERV, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o IPSERV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É vedado o compartilhamento de login para funções de administração de sistemas.

A área de tecnologia de informação responde pela criação da identidade lógica dos servidores na instituição.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

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.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade do IPSERV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É vedado todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor da área de tecnologia de informação, ou de quem este determinar.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes às atividades do IPSERV não deverão ser copiados movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do IPSERV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de tecnologia da informação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os servidores devem informar qualquer identificação de dispositivo estranho conectado ao seu computador;

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela área de tecnologia de informação ou por terceiros devidamente contratados para o serviço;

- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;

- O servidor deverá manter a configuração do equipamento disponibilizado pelo IPSERV, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;

- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados;

- Todos os recursos tecnológicos adquiridos pelo IPSERV devem ter imediatamente suas senhas padrões (default) alteradas.

Situações em que é vedado o uso de computadores e recursos tecnológicos do IPSERV:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

- Burlar quaisquer sistemas de segurança;

- Acessar informações confidenciais sem explícita autorização do proprietário;

- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

8. PRIVACIDADE DA INFORMAÇÃO

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

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

- As informações são coletadas de forma ética e legal, com o conhecimento do segurado / beneficiário, para propósitos específicos e devidamente informados;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- 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;
- As informações somente são fornecidas a terceiros, mediante autorização prévia da Diretoria-Executiva ou para o atendimento de exigência legal ou regulamentar;
- 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.

9. DISPOSITIVOS MÓVEIS

O IPSERV deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pela área de tecnologia de informação, como: notebooks, smartphones e pendrives.

O objetivo é estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.

O IPSERV, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no IPSERV, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade do IPSERV e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação, autorização e sem a condução, auxílio ou presença de um servidor da área de tecnologia de informação.

O servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de tecnologia de informação.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pelo IPSERV, notificar imediatamente o seu gestor direto e a área de tecnologia de informação.

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao IPSERV e/ou a terceiros.

10. PROCEDIMENTOS DE BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência em etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do uso recomendado pelo fabricante.

Tempo de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 90 ou 120 dias, de acordo com a criticidade do backup.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

Os arquivos de backup devem estar disponíveis em servidores externos de arquivo, como segunda fonte.

11. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.

Nos termos da Política de Segurança da Informação, a CODIUB procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a imagem da instituição.

É recomendado o treinamento dos usuários em segurança da informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os funcionários e demais colaboradores sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários.

Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e manterem-se informados da situação.

Tais recomendações seguem as previsões contidas no Estatuto do Servidor Público do Município de Uberaba (Lei Complementar Municipal nº 392/2008), no Código Civil Brasileiro (Lei nº 10.406/2002) e na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ao servidor público ou funcionário colaborador poderá ser aplicada penalidade no caso de irregularidade comprovada.

De acordo com a infração cometida, conforme determinação legal, as punições poderão ser, dentre outras: comunicação de descumprimento, advertência, suspensão ou demissão por justa causa.

12. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do IPSERV, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes.

Sua elaboração e revisão deverão ser precedidos pelo responsável da CODIUB, sendo posteriormente aprovado por órgão superior competente.

As normas aqui descritas deverão sofrer alterações sempre que necessário, sendo que estas deverão ser registradas pela CODIUB, aprovada por órgão superior competente e divulgadas pela própria CODIUB, dentro da estrutura organizacional do IPSERV, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

A Política de Segurança da Informação sempre seguirá os preceitos dos seguintes atos normativos: Constituição Federal, Lei Federal nº 10.406/2002, Lei Federal nº 13.709/2018, Lei Federal nº 8.159/1991, Lei Federal nº 9.610/1998, Decreto- Lei nº 2.848/1940, Lei Complementar Municipal nº 392/2008, Código de Ética do Instituto de Previdência dos Servidores Públicos Municipais de Uberaba, bem como futuras alterações e legislações compatíveis com a matéria aqui tratada.

ANEXO - TERMO DE CIÊNCIA

TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI DO IPSERV – Instituto de Previdência dos Servidores Públicos Municipais de Uberaba – MG.

Declaro que recebi a Política de Segurança da Informação - PSI do IPSERV, estando ciente de seu conteúdo e da sua importância para o bom exercício funcional do próprio IPSERV.

UBERABA/MG, de de 2024.

Nome Completo:
Matrícula:
Assinatura: