PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas

A Política de Segurança da Informação (PSI), orienta e estabelece as diretrizes e Normas Administrativas para a proteção dos ativos de Informação e a prevenção de responsabilidade legal para todos os usuários e funcionários da Prefeitura Municipal de Echaporã.

Portanto deverá ser cumprida e aplicado em todos setores do Governo Municipal e Terceirizados.

PSI – Política de Segurança da Informação está baseada nas recomendações propostas pela norma ABNT NBR ISSO 27002:2005/IEC, LGPD Lei Federal 13709/2018, Lei Governo Digital 14129/2021 e Lei de Acesso à Informação (LAI) 12527/2011, se ajustando com código de prática para a gestão da segurança da informação e está de acordo com outras leis vigentes em nosso país.

Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso do órgão público, visando a orientação de nossos usuários e funcionários para a utilização dos ativos de tecnologia da informação disponibilizados em suas tarefas.

O mesmo encontra-se disponíveis no site da Prefeitura Municipal de Echaporã (www.echapora.sp.gov.br/Legislação/Planos Municipais).

Sumário

OBJETIVOS

Estabelecer diretrizes que permitam aos usuários e funcionários seguirem padrões de comportamento relacionados à segurança da informação adequando-se às necessidades da Administração Municipal e de proteção legal de dados e equipamentos da Prefeitura Municipal de Echaporã e os direitos do cidadão.

Estabelecer a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento em pleno âmbito.

Preservar as informações do Governo Municipal e cidadãos 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.

DIREITOS

Toda informação produzida ou recebida pelos usuários e funcionários como resultado da atividade profissional, artísticas e educacionais e administrativas pertence à Prefeitura Municipal de Echaporã em seu âmbito. As exceções devem ser explícitas e formalizadas em contrato ou documento formal a Administração Municipal.

Os equipamentos de informática, comunicação, áudio e segurança, sistemas e informações são utilizados pelos usuários e funcionários para a realização das atividades profissionais pertencem a Administração Municipal. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços, assim o responsável do setor de avaliar este uso também e ficando de responsabilidade do usuário qualquer dano causado a patrimônio público e a sua responsabilidade conforme lei.

Fica da Administração Municipal e setor responsável a responsabilidade que poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS

Para a uniformidade da informação, a Política de Segurança da Informação (PSI) deverá ser comunicada a todos os Usuários e Funcionários da Prefeitura Municipal de Echaporã fim de que a política seja cumprida dentro e fora dos Órgãos Públicos.

Haver uma junta multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Junta Segurança da Informação.

Tanto a Política de Segurança da Informação (PSI) quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Junta Segurança da Informação.

Deverá constar em todos os contratos da Prefeitura Municipal de Echaporã o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pelos órgãos públicos Municipais.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação Usuários e funcionários. Todos os Funcionários devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade (Anexo I).

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Departamento de TI e ele, se julgar necessário, deverá encaminhar posteriormente a Junta Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser Implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades digitais, em todos os pontos e sistemas em que o órgão público julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet (WIFIs) e outros, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela Prefeitura Municipal de Echaporã ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A Prefeitura Municipal de Echaporã exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários e Funcionários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta Política de Segurança da Informação (PSI) será implementada a Prefeitura Municipal de Echaporã por meio de procedimentos específicos, obrigatórios para todos os funcionários, independentemente do nível hierárquico ou função no órgão público, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação (PSI) e das Normas de Segurança da Informação e LGPD acarretará violação às regras internas administrativas e sujeitará o usuário ou funcionários às medidas administrativas e legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Funcionários em Geral

Entende-se por funcionário público toda e qualquer pessoa física, contratada ou prestadora de serviço por intermédio da Prefeitura Municipal de Echaporã, que exerça alguma atividade dentro ou fora dos órgãos públicos.

Será de inteira responsabilidade de cada funcionário, todo prejuízo ou dano que vier a sofrer ou causar Prefeitura Municipal de Echaporã ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2 - Dos Funcionários em Regime de Exceção (Temporários e Contratados)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Prefeitura Municipal de Echaporã (Anexo III).

A concessão 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 funcionário que o recebeu não estiver cumprindo as condições definidas no aceite.

3 - Dos Gestores de Pessoas ou Processos

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

Atribuir aos funcionários, 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 (PSI) da Prefeitura Municipal de Echaporã.

Exigir dos colaboradores a assinatura do Termo de Compromisso e 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 da Prefeitura Municipal de Echaporã.

Antes de conceder acesso às informações da administração municipal, exigir a assinatura do Acordo de Confidencialidade dos funcionários casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas de trabalho (Anexo III).

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional, Administrativa e Culturais.

4 - Dos Custos diante da Informação

4.1 - Da Área 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 funcionários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação (PSI), e em sua versão Educacional, Administrativa e Cultural, pelas Normas de Segurança da Informação complementares.

Os administradores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, troca de arquivos entre setores a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais 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.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente Cloud (Computação em nuvem), fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Prefeitura Municipal de Echaporã.

Manter cópia de todos os backups de sistemas, software, imagens e segurança em salvo em local predeterminado e sobre guarda da administração Municipal.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações da Prefeitura Municipal de Echaporã, nos ambientes totalmente controlados por ela.

O Departamento de TI deve ser previamente informado sobre o fim do prazo de contratos e dispensa de serviços de informação, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo prestador.

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

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

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação e internet 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 ou responsável do setor.

Proteger continuamente todos os ativos de informação da Administração Pública contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de uso após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente administrativo em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção administrativa, educacional e cultural, bem como em ambiente exclusivamente administrativo, exigindo o seu cumprimento dentro da Prefeitura Municipal.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

4.1.1 Das Secretárias e Diretorias

As secretárias e Diretoria responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais e equipamentos específicos.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Prefeitura, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da a Prefeitura Municipal de Echaporã.

Garantir que todos os Funcionários, estações e demais dispositivos com acesso à rede de internet, e ambientes de rede e outros operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI para, para gerar indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Prefeitura Municipal de Echaporã;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Prefeitura Municipal de Echaporã;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os Funcionários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

O uso da rede Wifi e local, fica de responsabilidade do gestor local a disponibilidade de acesso (senhas de acesso) a internet e uso dos equipamentos de tecnologia de informação, como também a solicitação do termo de responsabilidades dos usuários e funcionários públicos.

O terno deve ser aguardado em seus setores para futuro, consulta e segurança.

4.2 - Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo chefia**,** nomeados para participar do grupo pelo período de um ano.

A composição mínima deve incluir um funcionário de cada uma das áreas: Administrativa, Educação e Saúde.

Deverá Junta Segurança da Informação reunir-se formalmente pelo menos uma vez ano. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a Prefeitura Municipal de Echaporã.

A Junta Segurança da Informação poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao Junta Segurança da Informação:

- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- Propor alterações nas versões da Política de Segurança da Informação (PSI) e a inclusão, a eliminação ou a mudança de normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação (PSI) ou das Normas de Segurança da Informação complementares e legais.

5 - Monitoramento de Rede e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta Política de Segurança da Informação (PSI), bem como de sua versão Administrativa, a Prefeitura Municipal de Echaporã poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless (WIFI) 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, solicitação da Administração pública ou por determinação da Junta Segurança da Informação.

- 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.

6 - Correio Eletrônico

O objetivo desta norma é informar aos funcionários da Prefeitura Municipal de Echaporã quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Prefeitura Municipal de Echaporã é para fins corporativos e relacionados às atividades do funcionário ou usuário dentro da Administração Pública. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Prefeitura Municipal de Echaporã e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos usuários e funcionários o uso do correio eletrônico da Prefeitura Municipal de Echaporã:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico 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 da Prefeitura Municipal de Echaporã 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 qualquer uma das unidades da Prefeitura Municipal de Echaporã estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que: contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura Municipal de Echaporã;
- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

- 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)
- 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.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da Prefeitura
- Telefone (s)
- Correio eletrônico

7 - Internet

Todas as regras atuais da Prefeitura Municipal de Echaporã 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 Administração Pública 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, a Prefeitura Municipal de Echaporã, 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 Prefeitura Municipal de Echaporã, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede e internet, estejam eles em disco local, na estação ou em áreas privadas da rede ou em nuvem visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Prefeitura Municipal de Echaporã, ao monitorar a rede interna e externa, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer funcionário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao funcionário e ao respectivo gestor da pasta. 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 administração cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela Administração Pública aos seus funcionários, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada, não prejudique o andamento dos trabalhos nas unidades e tarefas diárias.

Como é do interesse da Prefeitura Municipal de Echaporã que seus funcionários estejam bem informados, 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 trabalho.

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

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

É proibida a divulgação 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 ou qualquer outra tecnologia correlata que venha surgir na internet.

Os funcionários com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades da Prefeitura

Municipal de Echaporã e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Departamento de TI.

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.

Qualquer software não autorizado baixado será excluído pelo Departamento de TI, e seu superior informado da irregularidade.

Os funcionários não poderão em hipótese alguma utilizar os recursos da Prefeitura Municipal de Echaporã para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de educacionais e relacionados ao desenvolvimento pedagógico.

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

Funcionários com acesso à internet não poderão efetuar upload (subida) de qualquer software ou documento, licenciado a Prefeitura Municipal de Echaporã ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os Funcionários não poderão utilizar os recursos da Prefeitura Municipal de Echaporã 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. Desde que sejam autorizados pelos Departamento de TI, Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos eventualmente autorizados pelo Superior do setor.

Porém, os serviços de comunicação instantânea (Facebook, Whatzap e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o superior requisite formalmente à Departamento de TI o bloqueio.

Não é permitido acesso a sites de proxy e Cloud Alternativos que não seja certificado com o Departamento de TI.

8 - Identificação

Os dispositivos de identificação e senhas protegem a identidade do usuários e funcionários, evitando e prevenindo que uma pessoa se faça passar por outra perante da Prefeitura Municipal de Echaporã ou terceiros.

O uso dos dispositivos 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 Tecnologia e deverá ser aplicada a todos os usuários e funcionários.

Todos os dispositivos de identificação utilizados na Prefeitura Municipal de Echaporã, como o número de registro dos funcionários, o crachá, as identificações de acesso aos sistemas, os certificados digitais e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

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 funcionário, a responsabilidade perante a Prefeitura Municipal de Echaporã e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do superior de uso compartilhado ele deverá ser responsabilizado.

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

O Departamento de Recursos Humanos da Prefeitura Municipal de Echaporã é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos funcionários.

O Departamento de TI responde pela criação da identidade lógica dos colaboradores na Administração Municipal, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

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

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de TI.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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

A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. O sistema crítico e sensível para a administração pública e os logins com privilégios administrativos devem exigir a troca de senhas a cada 45 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

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

9 - Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos Funcionários são de propriedade da Prefeitura Municipal de Echaporã, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da administração municipal, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelos setores responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico Departamento de TI, ou de quem este determinar.

Os setores que necessitarem fazer testes deverão solicitá-los previamente à Departamento de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor do sistema.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de TI mediante registro de chamado via canal de comunicação e-mail ou whatzapp.

A transferência 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 e autorização do superior imediato.

Arquivos pessoais ou não pertinentes ao administração pública (fotos, músicas, vídeos, etc..) não deverão ser copiados e movidos para os drives de rede ou em cloud, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos funcionários da Prefeitura deverão ser salvos em drives de bachups. 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 funcionários da Prefeitura 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 do Departamento de TI.

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

- Todos os computadores de uso individual deverão ter senha de para restringir o acesso de colaboradores não autorizados. Tais senhas serão enviadas pela Departamento de TI quando solicitadas, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao departamento TI qualquer identificação de dispositivo estranho conectado ao seu computador.

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de Informática e tecnologia para qualquer tipo de reparo que não seja realizado por um técnico Departamento TI ou por terceiros devidamente contratados para o serviço.
- Todos os routes internos ou externos devem ser removidos ou desativados para impedir a invasão e 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 da Administração Municipal.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos de tecnologia.
- O Funcionário deverá manter a configuração do equipamento disponibilizado pela Prefeitura Municipal de Echaporã, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da Administração Pública, assumindo a responsabilidade como custo diante de informações.
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de
- Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Prefeitura Municipal de Echaporã devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos funcionários, datas e horários de acesso, caso haja a perda destas informações o ossuário será responsabilizado, só á exceção quando houver defeito físico no equipamento.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura Municipal de Echaporã sendo sobre administrativa.

- 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 e administração pública.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers) sem ser para uso de registro e pela administração Municipal.

- 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.

10 - Dispositivos Móveis

A Prefeitura Municipal de Echaporã deseja facilitar a mobilidade e o fluxo de informação entre seus usuários e funcionários. 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 pelo Departamento de TI, como: notebooks, smartphones e Pendrives e outros.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários e funcionários que utilizem tais equipamentos.

A Prefeitura Municipal de Echaporã, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O Funcionário, 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 na Prefeitura Municipal de Echaporã, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo funcionário 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 da Prefeitura Municipal de Echaporã e aos seus usuários e funcionários deverá seguir o mesmo fluxo de suporte adotado pela administração pública aos outros equipamentos.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

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 e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de TI.

O funcionário deverá responsabilizar-se em não manter ou utilizar quaisquer programas ou aplicativos que não tenham sido instalados ou autorizados por um técnico Departamento de TI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela administração pública 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 usuário e funcionário como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do usuário e funcionário, no caso de furto ou roubo de um dispositivo móvel fornecido pela Prefeitura Municipal de Echaporã, notificar imediatamente seu gestor direto e o Patrimônio da Prefeitura.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O Funcionário 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 a Prefeitura Municipal de Echaporã e/ou a terceiros.

O Funcionário que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura Municipal e seus setores deverá submeter previamente tais equipamentos ao processo de autorização da Departamento de TI.

Equipamentos portáteis, como Smartfones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao usuários e funcionários pela Prefeitura municipal de Echaporã, terão que ter devida autorização do superior imediato, e terno de responsabilidade ficara do superior do setor.

11 - Datacenter e Servidores

O acesso ao Datacenter e Servidores somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter e Servidor, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio de logs.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter e Servidores por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do Superior do Departamento de TI, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter e Servidores deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso aos servidores, e salva no diretório de rede.

Nas localidades em que não existam funcionários da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Servidor, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um Funcionários Autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Servidor, bem como assinar o Termo de Responsabilidade.

O acesso ao Datacenter E servidores, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer funcionário responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter e Servidores.

Deverão existir duas cópias de chaves da porta do Servidor. Uma das cópias ficará de posse do coordenador responsável pelo Servidor, a outra, de posse do coordenador de infraestrutura.

O Datacenter e servidor deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Limpeza.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou
Inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter e Servidor somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos pelo Patrimônio.

No caso de desligamento de empregados ou Funcionários que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de funcionário autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

12- Monitoramento de Segurança

Para garantir Política de Segurança da Informação (PSI), bem como de sua versão Administrativa, a Prefeitura Municipal de Echaporã poderá:

- Implantar sistemas de monitoramento câmeras e alarmes e outros, para segurança dos patrimônios públicos e bens públicos e segurança interna e pública.
- A informação gerada por esses sistemas poderá ser usada para identificar usuários e pessoas em respectivos acessos efetuados em setores, prédios públicos, bem como segurança e preservação dos bens públicos.
- Só poderá tornar públicas as informações obtidas pelos sistemas de monitoramento, no caso de exigência judicial, solicitação da Administração pública ou por determinação da Junta Segurança da Informação.
- Todos os superiores dos setores que estiver acesso aos sistemas instalados são responsáveis pelas imagens e terão que preservar as mesmas, o sigilo, integridades e conficiodabilidade das mesmas.
- Todas as solicitações de qualquer imagens e logs, terão que preencher formulário padrão (Disponível no site www.echapora.sp.gov.br) e protocolar na Administração Municipal que será avaliado o pedido e disponibilidade das mesmas.
- Todas as imagens terão que ser pedidas em 72 horas no máximo da ocorrência, após isto teremos que verificar a disponibilidade das mesmas nos backups
- Qualquer solicitação terá que ter identificação do solicitante, dia, hora de referências, para busca das imagens.
- Realizar a qualquer tempo, inspeção física nos equipamentos de sua propriedade.
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso, e monitoramento.
- Todas as solicitações serão referentes a todos os sistemas de monitoramento câmeras e alarmes.
- O acesso Central de Monitoramento de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um Funcionários autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Servidor de Imagens, bem como assinar o Termo de Responsabilidade.
- O acesso na Central de Monitoramento, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

- Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar
- Autorização com antecedência a qualquer funcionário responsável pela administração do Monitoramento liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Servidores.
- Deverão existir duas cópias de chaves da porta do Monitoramento. Uma das cópias ficará de posse do coordenador responsável pelo Monitoramento, a outra, de posse do coordenador de infraestrutura.

13 - Sistemas de Ponto Eletrônico

Para garantir Política de Segurança da Informação (PSI), bem como de sua versão Administrativa, a Prefeitura Municipal de Echaporã poderá:

- Implantar sistemas de Ponto Eletrônico, para coleta de pontos diariamente.
- A informação gerada por esses sistemas poderá ser usada para identificar usuários e pessoas em respectivo controle de frequência no trabalho.
- Só poderá tornar públicas as informações obtidas pelos sistemas de ponto Eletrônico, no caso de exigência judicial, solicitação da Administração pública.

14 - 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 Funcionários 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 com 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 prazo recomendado pelo fabricante.
- É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.
- Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.
- É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.
- As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, em outro local não próximo do Datacenter.
- Os backups imprescindíveis, críticos, para o bom funcionamento da administração Pública. Exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.
- 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 nos termos do Procedimento de Controle de Backup e Restore.
- Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.
- Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.
- Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.
- Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de

infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

- Os funcionários responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custo diante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custo diante não poderá se eximir da responsabilidade do processo.

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a Segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura Municipal de Echaporã. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela Administração Municipal.