POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A informática tem como objetivo instrumentalizar a prestação do serviço público, propiciando uma melhor gestão dos recursos da CET e possibilitando a integração entre seus órgãos para troca de informações.

O uso da Tecnologia da informação na administração pública envolve grande acervo de recursos computacionais e informações que necessitam estar permanentemente protegidos contra acessos indevidos e adulterações.

Em contrapartida aos benefícios que a informatização oferece, existe a constante tentativa de exploração maliciosa das informações, tornando-se imprescindível o zelo pela segurança, evitando as vulnerabilidades que dão margem a invasões e outros incidentes que resultam em perda da confidencialidade, integridade e disponibilidade das informações.

Como parte de um conjunto de medidas de segurança, fica imprescindível a implantação de uma política de segurança da informação que defina diretrizes, normas, padrões e requisitos mínimos, nos diversos aspectos que envolvem, direta e indiretamente, o trânsito e o acervo de informações, salvaguardando a sua exatidão, independentemente de onde e como estejam armazenados.

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da CET – Companhia de Engenharia de Trafego de São Paulo para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

I. OBJETIVO

Definir e estabelecer uma estrutura e diretrizes de Segurança de Informação na CET que permitam aos Empregados, estagiários, prestadores de serviço e profissionais que atuam sob contrato junto a CET e que no exercício de suas atribuições fazem uso de informações de negócio ou administrativas tenham ciência e venham a cumprir as diretrizes estabelecidas neste documento normativo.

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

Preservar as informações da CET 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.

II. FUNÇÕES DA SEGURANÇA DA INFORMAÇÃO

A função de Segurança da Informação, no que se refere à administração dos acessos aos sistemas de informação, está distribuída entre:

- Superintendência de Tecnologia (STE), que tem por função regular e definir a área de segurança de informática, que concede os acessos aos indivíduos, seguindo esta Norma;
- A Superintendência de Recursos Humanos (SRH), que tem por responsabilidade das pessoas habilitadas a exercer funções regulares na organização; e
- As demais superintendências da empresa, que estabelecem processos de negócio, administrativos e definem papéis para seus Empregados, estagiários, prestadores de serviço, ou quaisquer outras entidades que fazem uso dos recursos computacionais da CET.

Dentro da área de Recursos Humanos, a segurança de informação inicia seu “ciclo de vida” no que se refere à autoridade de acesso concedida aos indivíduos. Caracteriza-se pela manutenção dos usuários (Inclusão, exclusão) por ocasião de admissão, desligamento de Empregados e/ou terceiros.

Deve também zelar pela existência dos direitos de acessos quando ocorrer os eventos: férias, vencimento e/ou alteração de contratos de trabalho, comunicações de alterações de cargo, entre outros.

A função da área de segurança de informática, dentro da área de Tecnologia, caracteriza-se pela operacionalização dos acessos e administração de permissões em função do perfil do usuário e necessidades de acesso.

A área de segurança de informática (infraestrutura), é responsável por associar as pessoas ao perfil e as autorizações de acesso aos sistemas, transações e processos automatizados.

III. RESPONSABILIDADES

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

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

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

A Política de Segurança de Informações não é somente um processo gerencial administrativo em implementação é também de responsabilidade de cada usuário e de todos simultaneamente.

DAS RESPONSABILIDADES ESPECÍFICAS

- Dos Colaboradores em Geral:
  Entende-se por colaborador toda e qualquer pessoa física, vinculada à CET (Empregados, Diretores, Estagiários e Menores Aprendizes) ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a CET e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

- Dos Colaboradores em Regime de Exceção (Temporários):
  Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pela Gerencia de Informática.

  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 colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

- Dos Gestores de Pessoas e/ou Processos:
  Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

  Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento das Normas de conduta da CET.

  Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência conforme previsto no Código de conduta CET, 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 CET.

  Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

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

IV. DOS CUSTODIANTES DA INFORMAÇÃO

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 colaboradores com todos os controles necessários para cumprir os requerimentos de segurança

estabelecidos por esta PSI, pelas Normas de Segurança da Informação complementares.

Os administradores e operadores 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, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, 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.

Garantir segurança especial para sistemas com acesso público, 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 CET.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

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, 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 Empregados serão de responsabilidade do próprio Empregado; e
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso e determinar que sejam aplicados testes e verificações adequadas, buscando garantir essa proteção contra código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa 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 corporativo.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

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

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

Monitorar o ambiente de TI, gerando 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 CET;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da CET;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e
- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

V. GESTORES DE ÁREA

Os gestores devem assegurar que as normas e procedimentos da Política Corporativa de Segurança de Informações, sejam implementadas e mantidas de acordo com os

preceitos definidos, para as suas áreas de atuação, além disso, devem dar o exemplo na aplicação dessas normas e procedimentos.

Devem assegurar que todos os subordinados estejam cientes do que é esperado deles, e que, ajam sensivelmente de modo a proteger a informação, e encorajá-los a informar qualquer tipo de problema que venha a ocorrer e possa colocar em risco as informações.

Devem estar conscientizados dos riscos associados com a perda da confidencialidade, integridade e disponibilidade das informações (Código de conduta CET).

VI. EMPREGADOS, ESTAGIÁRIOS E MENORES APRENDIZES

Todos os Empregados, estagiários e menores aprendizes têm por responsabilidade conhecer essa Política e cumpri-la integralmente no dia a dia, deve participar de programas de conscientização de segurança, assim que for admitido, deve utilizar equipamentos e serviços para os quais tenha sido autorizado e devidamente orientado, deve conhecer suas responsabilidades específicas sobre segurança e cumpri-las rigorosamente e somente utilizar os serviços para os quais tenha permissão.

VII. PRESTADORES DE SERVIÇOS

O acesso de prestadores de serviços aos recursos de tecnologia da informação da CET deve basear-se sempre em contrato formalizado entre as partes.

A empresa prestadora de serviços deve garantir, por seus Empregados, a observância das Normas de Segurança de Informações estabelecidas na CET.

Todo contrato deve possuir, dentre outras, cláusulas que assegurem a confidencialidade da informação e sua auditoria.

Acordos formais devem ser firmados para o intercâmbio (eletrônico ou manual) de dados entre a CET e demais empresas. Tais acordos visam garantir que tanto as informações da CET quanto da outra empresa recebam externamente a mesma proteção que recebem internamente.

É obrigatória a colaboração das áreas solicitantes dos serviços quando a contratação oferecer riscos de violação da Política de Segurança da Informação e a previsão pela área técnica responsável das obrigações e penalidades que assegurem o cumprimento desta Política.

VIII. REVISÃO DE ACESSO

Periodicamente, a área de Segurança da Informação envia um relatório extraído dos sistemas/aplicativos com os perfis dos Empregados/prestadores de serviços para os Gerentes de cada área (responsáveis pelos devidos sistemas da CET).

Este processo é chamado de Revisão de Acesso, e tem o propósito de validar cada acesso existente nos sistemas da empresa, mantendo ou solicitando a revogação do mesmo.

A periodicidade da revisão depende da criticidade do sistema em questão: para aqueles chamados de críticos, a frequência das revisões é semestral ou de acordo com o definido. Para os demais sistemas da companhia, as revisões ocorrerão anualmente.

Tão logo o Gerente de área responsável da Informação retorne a revisão à área de segurança de informática executa as alterações solicitadas, comunica o gerente e finaliza a revisão.

A validação do acesso do gerente responsável da informação poderá ser feita por ele mesmo, quando não houver um superior na hierarquia da área. Por exemplo, podendo ser o diretor da área.

IX. CONTROLE DE ACESSO AOS SISTEMAS DE INFORMAÇÃO

A primeira linha de defesa para proteção contra acesso não autorizado é a identificação do usuário, via controle de autenticação de acesso. O processo de autenticação é realizado pela combinação de dois fatores: **identificação do usuário e senha**.

A identificação do Usuário e sua respectiva senha são à base do processo de proteção. Cabe a todos os Empregados, estagiários e prestadores de serviço sob contrato a compreensão de que cuidar e manter em segredo sua senha de acesso é fundamental para que os outros controles possam ser exercidos.

Na CET, existem agrupamentos dos acessos baseados nas funções dos colaboradores da empresa, os quais podem ser chamados de Perfil por Função. Este mapeamento de funções visa disponibilizar todos os acessos pertinentes a determinado cargo, necessários para que um novo colaborador possa desempenhar suas atividades.

Desta forma, na admissão, o Empregado receberá os acessos definidos via Perfil por Função correspondente, baseados nas informações de área e cargo, sem a

necessidade de aprovações específicas, pois foram previamente autorizados pelo gestor responsável quando da definição do perfil.

Exceto quando o Perfil por Função atribuído ao cargo/área do solicitante já inclua a permissão de acesso, os seguintes documentos deverão ser preenchidos e utilizados na formalização/autorização do acesso solicitado:

DOCUMENTO	REQUERIDO PARA	FINALIDADE DO TERMO	NÍVEL DE APROVAÇÃO PARA A CONCESSÃO DO ACESSO
Controle de acessos a recursos de TI.	Empregados / Terceiros	1) Autorizar o acesso à VPN. 2) Autorizar o acesso aos bancos de dados da empresa. 3) Autorizar o acesso aos bancos de dados de produção. 4) Autorizar acesso a dispositivos móveis. 5) Permitir a administração local de equipamentos.	Área de TI – Superior imediato, com ciência do Coordenador de Segurança da Informação. Demais Áreas – Superior imediato (cargo mínimo gerente) e Coordenador de Segurança da Informação.
Termo de Responsabilidade de Função Especial	Empregados	Dar ciência da responsabilidad e atribuída à função assumida.	Gerente e/ou Superintendente do solicitante e Coordenador de Segurança da Informação.
Termo de Responsabilidade de Prestador de Serviços	Terceiros	Dar ciência das Normas e Políticas da CET e declarar responsabilidade assumida.	Gestores responsáveis

Nenhum acesso será concedido sem a prévia autorização, conforme definido.

X. SENHAS

A senha é de uso pessoal e exclusivo e seu usuário deve mantê-la confidencial, a primeira senha fornecida ao usuário, deve ser trocada imediatamente no primeiro logon, serão trocadas em intervalos definidos em frequência menor quando a aplicação assim o exigir.

As senhas são mantidas de forma criptografada, não sendo permitido o acesso ao arquivo de senhas. Estas podem ser reativadas, mas nunca visualizadas.

Os sistemas de informação da empresa e os recursos de administração (que definem quem pode acessar quais informações) são os principais instrumentos de gestão de segurança. A área de segurança de informática (infraestrutura) é responsável pela aplicação das regras de acesso e a administração destes recursos.

Cada sistema reflete a segurança do ambiente onde processa. Todo acesso é iniciado pela identificação via software de gerenciamento da rede local, onde o microcomputador está ligado. Uma vez feita à identificação, via login/senha, a pessoa terá ou não acesso aos recursos sistêmicos.

Os colaboradores fazem uso dos sistemas após a identificação (login/senha) na Rede Local. Esta é a mais importante forma de controle sobre os ativos de informática, uma vez que esta é a “chave- única” comum a todos os sistemas, independentemente de localidade. Todos precisam zelar pela confidencialidade de sua senha acima de tudo.

XI. CUIDADOS COM A SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DOS EQUIPAMENTOS – COMPUTADORES

Os ativos de tecnologia (hardware e software) devem ser claramente identificados por meio de inventário de ativos, que deve ser efetuado no mínimo anualmente.

Os ativos de tecnologia não podem ser instalados e ou alterados. Exceções devem ser tratadas pela área de Infraestrutura Tecnológica.

Devem ser utilizadas somente conexões aprovadas (ex.: gateways, proxy, firewalls).

Não é permitido o acesso remoto sem a devida autenticação do usuário (identificação do usuário e senha), com a CET estabelecendo o mecanismo de autenticação que será usado no acesso à rede.

Os equipamentos utilizados fora das instalações da CET, cuja utilização tem o propósito de dar suporte a atividades ligadas ao negócio, devem estar sujeitos à autorização prévia dos Gestores e da área de Infraestrutura Tecnológica, seguindo as recomendações.

Microcomputadores só podem ser utilizados se tiverem um antivírus instalado, o qual é automaticamente atualizado quando do acesso à rede. O antivírus é mantido permanentemente atualizado pela área de Suporte ao Usuário Final. Em nenhuma hipótese poderão ser desligados ou inativados.

Cabe à área de Suporte ao Usuário Final a formatação do equipamento para garantir que nenhum programa ou dado seja enviado junto com o equipamento. A doação limita-se somente ao hardware. O software não poderá ser doado, pela sua natureza de licenciamento sem direito de transferência.

Para garantir a eficácia dos procedimentos a CET se reserva no direito de:

- Implantar softwares e sistemas que possam monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa; e
- Inspecionar qualquer arquivo armazenado na rede, ou que estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta Política de uso.

Os recursos de tecnologia e os ativos de informação da CET devem estar protegidos contra-ataques de vírus, invasões e operações externas ou internas que exponham os ativos a perda de integridade ou outros riscos.

Todos os computadores da CET possuem Antivírus; os quais nunca deverão ser retirados e/ou desabilitados.

A informação classificada (secreta ou confidencial) deve ser armazenada em diretórios de servidores que possuem backup automático, mas nunca em diretórios locais (ex.: drive C:\) das estações de trabalho.

Não são permitidas alterações na configuração física ou lógica dos recursos de tecnologia da Companhia. Exceções serão tratadas pela Gerência de Informática.

Todas as conexões da rede interna da CET com redes externas operam por meio de implementações seguras e monitoradas, com roteadores e firewalls, a geração de eventos de segurança (log) deve estar sempre ativa e deve ser periodicamente analisada.

O tempo de conexão dos usuários deve ser restrito principalmente em áreas e/ou aplicações de alto risco.
Procedimentos formais devem ser conduzidos para gerenciar o acesso à informação, como:

- Registro de novos usuários;
- Gerência de senhas de usuários; e
- Reavaliação ou revogação de acesso.

Os componentes de identificação do usuário e senha são de uso pessoal e exclusivo do titular.

As aplicações devem operar com base na identificação do usuário para liberar acesso a um sistema, em vez da identificação da estação de trabalho.

A identificação de usuários não pode apresentar indicação de direitos de acesso, ou seja, não deve haver maneira de se identificar se determinado user ID pertence a um gerente, supervisor ou administrador de rede, dentre outros.

Os acessos a dados confidenciais devem ser feitos sempre por meio de um aplicativo, nunca diretamente pelo usuário.

Qualquer acesso a aplicações deve ser precedido de autenticação e controle de acesso a recursos, de modo a permitir rastreamento das operações realizadas.

As estações de trabalho ou terminais devem ser protegidas contra uso não autorizado, por meio de dispositivo de bloqueio, quando não estiverem em uso.

A proteção de tela (screen saver) deve ser utilizada com senha, para garantir a segurança e a confidencialidade das informações.

Os sistemas operacionais de os desktops / laptop, aplicativos de software deverão ser transferidos para os novos equipamentos e os equipamentos substituídos deverão ser inutilizados de acordo com o processo de descarte e não poderão ser utilizados após o término de sua vida útil.

O conjunto padrão dos aplicativos de desktop / laptop, estabelece que os aplicativos devem ser compatíveis, configurados e testados para suportar as funções dos negócios.

Os controles básicos dos sistemas, bem como as Políticas e Procedimentos devem ser adotados para prevenir a instalação no computador de materiais registrados que

possuam ferramentas automáticas de auditoria e que podem coletar informações de instalação do aplicativo. Isso também é valido para softwares padrão. Usuários finais não devem possuir nenhum direito ou privilégios de Administrador em seus computadores.

Tais procedimentos devem ser adotados para garantir o suporte eficiente às questões relacionadas aos usuários, a fim de manter os níveis segurança definidos pela empresa na disponibilização dos Desktop/Laptop.

Para assegurar a oportuna resolução dos problemas e solicitações dos usuários finais, é necessário o gerenciamento centralizado e automatizado das implantações de manutenção/consertos, correções, pacote de serviços, etc.

A documentação da política deve ser armazenada, juntamente com os dados do negócio, em um servidor de backup e não localmente em um Desktop/Laptop.

Devem ser adotados procedimentos para garantir o suporte eficiente com as questões relacionadas aos usuários finais, a fim de manter os níveis segurança definidos pela empresa na disponibilização do Desktop/Laptop.

O usuário deve fazer manutenção periódica no diretório de armazenamento dos arquivos, para evitar acúmulo de arquivos inúteis.

XII. PROCEDIMENTOS DE OPERAÇÃO DOS EQUIPAMENTOS

Esse tópico visa definir as normas de utilização de rede e engloba o login, manutenção de arquivos no servidor corporativo e estações de trabalho e regras de acesso.

É proibida qualquer tentativa de se obter acesso não autorizado: tentativa de fraudar autenticação ou segurança de qualquer servidor, rede ou conta.

É proibida qualquer tentativa de interferir nos serviços de qualquer servidor, rede ou outro usuário. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um Servidor e tentativas de "quebrar" (invadir) um Servidor.

É proibido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários.

Diretório no Servidor de Arquivos: Cada área tem um diretório (espaço) no servidor e um limite de armazenamento.

O acesso a esse diretório será apenas para os usuários pertencentes à mesma área, caso haja a necessidade de disponibilizar o acesso para outros usuários não pertencentes aos mesmos departamentos, deverá ser aberto um chamado via HELPDESK, que será avaliado pelas áreas envolvidas nesse processo.

Gerenciamento de Diretório (espaço) no Servidor de Arquivos: Cada área será responsável pelo gerenciamento de seu diretório no Servidor de Arquivos, apagando arquivos duplicados e arquivos que não estão sendo mais utilizados. Caso seja necessário manter estes arquivos por mais tempo, deverá ser aberto um chamado via HELPDESK, para a Área de Produção TI responsável por realizar o backup do Servidor de Arquivos. Após a confirmação da realização do backup os mesmos deverão ser apagados.

Por medida de segurança, é aconselhável o armazenamento de todos os arquivos importantes inerentes à CET no Servidor de Arquivos, como garantia de backup, ou seja, os arquivos não devem ser armazenados na estação de trabalho.

O acesso e as aprovações às pastas de rede se darão de forma automática através de sistema, onde os respectivos Gerentes de áreas já estão cadastrados.

É proibida a edição, distribuição ou exposição e armazenamento de qualquer material que viole qualquer lei ou regulamentação em vigor no território nacional, tais como:

- Material de qualquer natureza com apoio ao racismo, nazismo ou discriminação;
- Material protegido por copyright, marcas registradas;
- Segredo comercial ou qualquer direito de propriedade intelectual usado sem a devida autorização;
- Material obsceno, material difamatório, que constitua uma ameaça ilegal, Pedofilia ou qualquer outro ato descrito pela legislação nacional como crime; Arquivos com as extensões: .pst, .pab, .eml, .msg,.idx, .mbx, .mmf, .aif, .asf, .au, .avi, .htm, .m3u, .mid, .midi, .miv; .mov, .mp2, .mp3, .mp4, .mpe, .mpeg, .qt, .mi, .snd, .wav, .wm,.wma, .wmv, .mp3a, .mp3b, .mp33; e
- Utilização do servidor de arquivos para distribuição e gravação de programas, aplicativos: filmes, vídeos, arquivos de áudio, executáveis e jogos.

Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.

É proibida a instalação ou remoção de softwares dos equipamentos da Companhia. Havendo necessidade, a área interessada deverá efetuar a abertura de chamado via HELPDESK.

É proibida a abertura pelo usuário de computadores ou outro componente físico da rede para qualquer tipo de reparo, à exceção para troca de suprimentos (cartucho de tinta, papel etc.); caso seja necessário o reparo o interessado deverá efetuar a abertura de chamado via HELPDESK.

É proibida qualquer alteração de configurações de rede e inicialização das máquinas bem como das estações de trabalho. Tratam-se de parametrizações que garantem a integridade e eficiência da rede.

É proibido o acesso à rede lógica da CET por um usuário utilizando o acesso fornecido por outro Empregado.

É proibido aos Empregados, o acesso aos sistemas/aplicativos da CET com equipamentos próprios.

XIII. UTILIZAÇÃO DE ACESSO À INTERNET

O acesso à internet é poderosa e efetiva ferramenta de negócio. Entretanto, pode causar sérios riscos aos recursos de tecnologia da empresa, quando utilizado de forma inapropriada. Para minimizar esse risco, os usuários são responsáveis por seu uso correto, inclusive, mas sem limitação, pelo cumprimento de todas as normas e procedimentos aplicáveis.

O acesso à Internet na CET é feito através das mesmas redes de comunicação que os sistemas se utilizam. Dessa forma, todos os usuários precisam estar cientes da carga que provocam na rede quanto ao acesso à Internet.

A internet deve ser utilizada para minimizar custos e maximizar o valor e a produtividade dos negócios da empresa.

É proibido utilizar os recursos da CET para fazer o download ou distribuição de software ou dados não legalizados.

São proibidas Baixas (download) de softwares ou aplicações da internet (freeware ou shareware). Exceções serão tratadas pela área de Suporte ao Usuário Final.

É proibido copiar, revelar, transferir, examinar, renomear, trocar ou deletar informações ou programas pertencentes à CET ou ao proprietário da informação.

O uso da internet deve priorizar as atividades relacionadas aos negócios e serviços da empresa, à comunicação com clientes e fornecedores, às pesquisas de tópicos

pertinentes e à obtenção de informação empresariais úteis, com a finalidade de manter os níveis mais altos de produtividade, qualidade e atualização técnica; O uso da internet para atividades pessoais deve ser restrito para casos excepcionais.

É proibida qualquer atividade que interrompa ou comprometa a integridade e a segurança dos recursos de computação e comunicação, ou que, de outra maneira, resulte em seu uso impróprio, comprometendo o desempenho do ambiente de tecnologia da CET.

Serão monitorados e armazenados todos os arquivos (log) gerados pelos mecanismos que viabilizam os serviços de internet, para posterior análise e verificação do cumprimento da Política e Normas Corporativas de Segurança Informações pelas áreas de competência.

Quando da percepção de qualquer falha de segurança ou do recebimento inadvertido de informações de origem desconhecida, a área de Informática ou o superior imediato deve ser avisado imediatamente.

Um software antivírus é mantido ativo e atualizado nas estações de trabalho ou em equipamento notebook interligado à rede da empresa.

Qualquer ocorrência registrada por intermédio de acesso concedido, no período após o desligamento do Empregado ou estagiário possuidor de tal acesso, será de responsabilidade da chefia da área correspondente.

Haverá geração de relatórios dos usuários e se necessário à publicação desse relatório.

Não será permitida a utilização de aplicativos P2P. (peer to peer, ponto a ponto rede de computador que compartilham arquivos pela internet).

Não será permitida a utilização de serviços, como: sites de músicas, jogos, redes sociais, streaming de filmes/series e afins.

O uso de ferramenta de mensagem instantânea não corporativa não é permitido, exceções deverão ser aprovadas e sua necessidade de negócio deve ser justificada.

XIV. UTILIZAÇÃO DE E-MAIL

O sistema de correio eletrônico da CET deve ser utilizado apenas para fins profissionais, de forma individual e discriminada, por intermédio exclusivo do software homologado pela área de TI.

É obrigatória a utilização de assinatura (identificação) nos e-mails com o seguinte formato: Nome do Funcionário, Empresa, Função, Telefone Comercial, E-mail e **Logotipo da CET**, sob orientação da Companhia (Marketing ou Diretoria Plena). (Por exemplo Aviso Geral 019/20).

XV. ADMINISTRAÇÃO DE SERVIDORES

No gerenciamento dos servidores devem estar previstos os seguintes procedimentos:

- Ativação e desativação de equipamentos;
- Backup de dados;
- Manutenção de equipamentos;
- Service Level Agreement – SLA;
- Plano de Contingência;
- Configuração e administração do ambiente de tecnologia;
- Controle de acesso ao Data Center, salas de comunicação, roteadores, switches; e
- Reinicialização e recuperação.

As atividades e o estado da rede devem ser monitorados, com relação a possíveis problemas e ao planejamento da capacidade dos equipamentos.

XVI. ACESSO REMOTO (VPN)

Todo acesso remoto (VPN) só pode ser feito através de um equipamento da CET.

A diretoria/superintendência/gerência/depto. envia solicitação de VPN para o Empregado para o e-mail cadastrovpn@cetsp.com.br com as seguintes informações:

Área	Nome completo	Registro	Login	E-mail particular	Telefone Celular	Patrimônio Micro CET que será acessado

O Grupo de Suporte recebe esse e-mail, cadastra as informações do usuário em uma planilha que está no servidor de arquivos com permissão apenas para o grupo.

Para os cargos que utilizam o acesso remoto como parte de seu trabalho, o acesso é “default”, ou seja, já faz parte do perfil, não havendo necessidade de aprovação.

São cargos autorizados: Presidente, Diretores, Superintendentes, Auditores, Gerentes, Analistas de Sistemas/Desenvolvedores, Analistas de Produção e Infraestrutura de TI (exceto Help Desk), que exerçam atividades externas onde há necessidade de acesso remoto.

Para os Empregados/colaboradores que exerçam atividades HOME OFFICE o acesso remoto deverá ser “default” ou seja, já faz parte do perfil, não havendo necessidade de aprovação.

Para os cargos que utilizam Notebook cedidos pela CET (mobilidade de acesso) como parte de seu trabalho, o acesso remoto deverá ser “default”, ou seja, já faz parte do perfil, não havendo necessidade de aprovação.

XVII. A SEGURANÇA DENTRO DO SISTEMA CORPORATIVO

A Política de Segurança está implantada dentro do Sistema Corporativo através de recursos que liberam o acesso as atividades, às atividades que vai desempenhar utilizando-se das funcionalidades dos sistemas, de forma que deve haver no mínimo controles e registros:

- Usuários: Cada ocorrência é um indivíduo. Registra recursivamente toda a hierarquia da empresa até o nível mais alto que é o Presidente, ou seja, todas as pessoas estão ligadas nesta hierarquia;
- Grupo-Usuário: Agrupamento das pessoas;
- Privilégio-Grupo: Relaciona para cada Grupo a autoridade de Consultar ou realizar Manutenção; e
- Privilégio-Usuário: Relaciona para cada Pessoa uma exceção de autoridade em relação à tabela Privilégio Grupo.

Esta estrutura reflete as funções de negócio que podem ser implementadas “dentro” do sistema, suas subfunções organizadas por natureza e também o “lado organizacional”, ou seja, quem vai executar estas funções.

XVIII. FORMAS DE ACESSO SEM UTILIZAÇÃO DOS SISTEMAS DE INFORMAÇÃO

Algumas áreas para realizar seu trabalho requerem acesso às bases de dados de maneira não- repetitiva ou passível de programação e inclusão em sistemas. Essa ferramenta permite acesso exclusivo para leitura (jamais com ação modificativa, inserção ou exclusão de dados).

A área de Desenvolvimento e Manutenção de Sistemas, no desempenho de suas atividades utiliza essa ferramenta para ler (exclusivamente) conteúdo dos bancos de dados e verificar a correção dos processos sistemas ou assistir as áreas de negócio nas investigações de qualquer anormalidade (trouble-ticket).

Nenhuma outra área, pode usar essa ou outra ferramenta a não ser com autorização específica fornecida pela área de TI.

XIX. DESENVOLVIMENTO SEGURO DE SISTEMAS

Os projetos que envolvam desenvolvimento de sistemas devem ser conduzidos de maneira controlada e segura, seguindo boas práticas de gestão do PMI e/ou metodologia ágil para o gerenciamento do desenvolvimento de sistemas. Toda documentação gerada no projeto deve ser armazenada e compartilhada com os envolvidos no projeto, de acordo com as recomendações da metodologia utilizada.

Os programas fontes e/ou compilados que estejam em fase de desenvolvimento ou manutenção devem ser mantidos em bibliotecas do ambiente de desenvolvimento, utilizando ferramenta para controle de versão e possibilidade de recuperação em caso de falhas.

Controles de segurança devem ser planejados e definidos na fase de análise de requisitos do desenvolvimento de um sistema, de forma a fazer parte do sistema desde o início de sua implementação.

A documentação dos sistemas deve conter informações específicas sobre os controles de segurança, de maneira que os usuários fiquem cientes de sua existência; O acesso a sistemas, aplicações e bases de dados necessários à condução de um trabalho deve ser restrito a coordenadores, analistas e programadores.

A definição dos controles de segurança deve considerar as seguintes necessidades:

- Controlar o acesso aos ativos da informação, inclusive requisitos de segregação de tarefas e ambientes
- Produzir trilhas de auditoria; quando necessário;
- Verificar e proteger a integridade de dados críticos;
- Proteger a informação contra acesso não autorizado;
- Utilizar criptografia para proteger dados críticos de negócio, quando transmitidos ou armazenados, se possível;
- Proteger a informação contra modificação não autorizada;
- Estar em conformidade com requisitos legais, fiscais, contratuais etc.;
- Realizar, no mínimo, cópias backup dos dados críticos do negócio;

- Recuperar falhas, especialmente em sistemas com requisitos de alta disponibilidade;
- Habilitar o sistema a ser operado e usado de forma segura por pessoal não especializado, porém treinado;
- Para toda aplicação desenvolvida, validar a entrada de dados, com o intuito de garantir a integridade dos dados manipulados pela aplicação;
- Para todo sistema desenvolvido, devem ser incorporados mecanismos de proteção contra falhas de processamento e contra atos intencionais que possam alterar indevidamente os dados manipulados pelo sistema;
- Para todo sistema desenvolvido que envolva transmissão de mensagens, deve ser feita análise dos riscos de segurança, para determinar se é legítimo ou não o emprego da técnica de autenticação de mensagens e, em caso afirmativo, qual o melhor método de implementação da técnica;
- Deve ser evitado o uso de dados reais no processo de teste dos sistemas;
- Nenhum processo de desenvolvimento de sistemas deve alterar informações dos ambientes de produção;
- Os sistemas desenvolvidos devem passar por um processo completo de testes e de controle de mudanças, antes de serem liberados à produção;
- Os códigos-fonte de programas devem ser devidamente controlados e armazenados em local seguro;
- Os ambientes de desenvolvimento e manutenção devem ser estritamente controlados, de modo a garantir que as mudanças sejam revistas, segregadas e aprovadas, antes de efetuadas no ambiente de produção; e
- A passagem de um novo programa ou sistema, ou alterações nos programas ou sistemas existentes, do ambiente de testes para o de produção deve ser rigorosamente controlada, explicitamente autorizada por pessoas distintas e devidamente documentada.

XX. DISPOSITIVOS REMOVÍVEIS

O acesso aos dispositivos de armazenamento removíveis para Empregados e colaboradores somente poderá ser realizado conforme procedimentos abaixo:

- O Empregado/colaborador solicitante declara estar ciente da responsabilidade pelo acesso ao(s) dispositivo(s) de armazenamento removível (is) solicitado(s) e assume toda e qualquer responsabilidade pelo seu uso e pelo uso das informações por ele(s) transitadas; e
- O Diretor do solicitante e o Coordenador de Segurança da Informação, autoriza o Empregado a ter acesso ao(s) dispositivo(s) e afirma que este recebeu todas as instruções para o correto uso do(s) dispositivo(s) quanto à confidencialidade das informações que serão utilizadas, sobre o uso exclusivo para fins

profissionais e sobre a Norma Institucional que trata do assunto sobre segurança das informações.

Para os cargos que utilizam o dispositivo de armazenamento removível como parte de seu trabalho devido ao uso de equipamentos cedidos pela CET (máquina fotográfica, notebook e telefone móvel), o acesso é “default”, ou seja, já faz parte do perfil, não havendo necessidade de aprovação.

São cargos autorizados: Presidente, Diretores, Superintendentes e Gerentes \supervisores que exerçam ou não, atividades externas onde há necessidade de acesso do dispositivo de armazenamento removível.

XXI. ADMINISTRAÇÃO DE LICENÇAS DE SOFTWARES

Todo software instalado deve possuir licença válida de uso.

A área de Infraestrutura Tecnológica é responsável por manter/controlar as licenças dos softwares instalados, efetuando o gerenciamento dessas licenças de software adquiridas e utilizadas, para estar em conformidade com a legislação.

Nenhum software deve ser copiado, exceto nos casos especificados nos termos de licenciamento e previamente autorizados pela área de Infraestrutura Tecnológica.

Nenhum software adquirido de terceiros ou desenvolvido internamente pode ser instalado ou utilizado, sem antes ser homologado pela área de Infraestrutura Tecnológica.

Toda instalação de software deve ser realizada ou reconhecida pela área de Infraestrutura Tecnológica.

Nenhum software, mesmo freeware, deve ser instalado no ambiente de rede da CET.

A distribuição e o controle dos softwares na CET são feitos através de ferramenta a qual permite a emissão do inventário.

O inventário dos softwares, deve ser mantido sempre atualizado, o que concorrerá para a proteção efetiva, tornando-se a base para a realização da classificação da informação e para a atribuição da propriedade desses ativos.

XXII. VÍRUS E SOFTWARES MALICIOSOS

O software de antivírus deve examinar todos os arquivos, em busca de vírus conhecidos, tão logo servidores, estações de trabalho e equipamentos stand alone

sejam ligados, permanecendo ativo durante todo o período em que o equipamento estiver ligado, visando identificar qualquer comportamento estranho de determinado sistema ou aplicação.

Antes da instalação de qualquer arquivo ou software recebido de terceiros ou parceiros no ambiente de produção, ele deve ser examinado.

Todo arquivo ou mídia recebidos de fonte externa deve ser checado com relação à existência de vírus, antes de ser utilizado e/ou enviado a outro destino.

Somente mídias e softwares licenciados e homologados são instalados na rede CET pela área de Informática.

O boot pelos drives externos é restrito ao pessoal de Suporte.

É proibido abrir arquivos executáveis recebidos via e-mail.

O controle de acesso interno e externo à rede CET é assegurado por meio de firewall; qualquer incidente deve ser prontamente comunicado à área de Tecnologia.

O backup dos dados mantidos em servidores é realizado regularmente.

XXIII. REFERENCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT).
NBRISO/IEC27001, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos, março de 2006.

ABNT. NBRISO/IEC27002, Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, agosto de 2005.

ABNT. NBRISO/IEC27005, Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação, julho de 2008.

APROVAÇÃO
Conselho de Administração da CET
Em 28 de setembro de 2021

DIVULGAÇÃO
Permanente