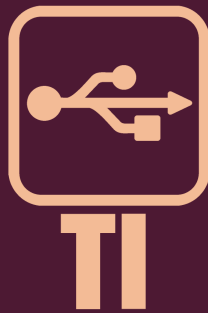
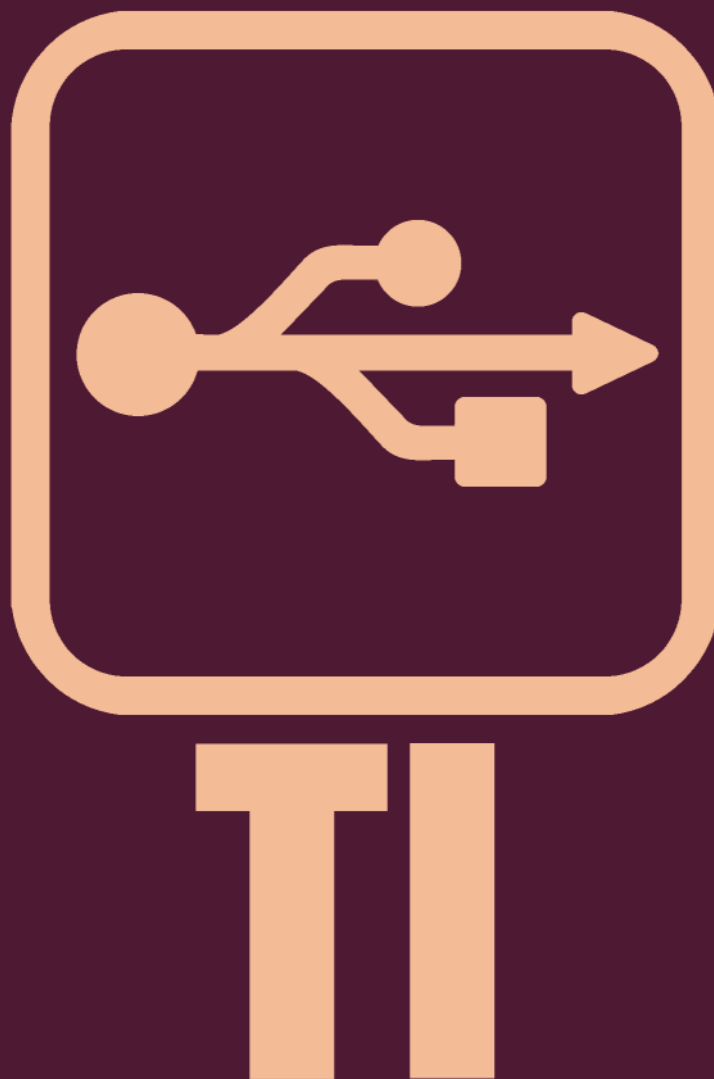


MANUAL DE SEGURANÇA DA INFORMAÇÃO



Departamento de Tecnologia
da Informação do Ipem-SP





Manual de segurança da informação

Créditos

Criação e desenvolvimento: *Departamento de Tecnologia da Informação do Ipem-SP*

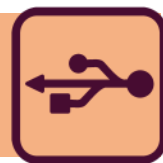
Projeto gráfico, diagramação e editoração: *Assessoria de Comunicação Social do Ipem-SP*

Instituto de Pesos e Medidas do Estado de São Paulo - Ipem-SP

Rua Santa Cruz, 1922 - São Paulo - Ouvidoria: 0800.013.05.22 - www.ipem.sp.gov.br

Esta é uma publicação do Instituto de Pesos e Medidas do Estado de São Paulo criada e desenvolvida pelo Departamento de Tecnologia da Informação para ser divulgada exclusivamente em ambiente virtual.

Janeiro de 2021



SUMÁRIO

APRESENTAÇÃO	4
PORTARIA IPEM-SP Nº 148 DE 14 DE DEZEMBRO DE 2020	5
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO (P-SI-001)	7
CLASSIFICAÇÃO, ROTULAGEM E MANUSEIO DA INFORMAÇÃO (N-SI-001)	17
USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO (N-SI-002)	24
GESTÃO DE IDENTIDADE E CONTROLE DA ACESSO (N-SI-003)	31
ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS (N-SI-004)	38
USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS (N-SI-005)	42
PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS (N-SI-006)	48
USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS (N-SI-007)	52
ACESSO REMOTO (N-SI-008)	55
MONITORAMENTO DE ATIVOS E SERVIÇOS DE INFORMAÇÃO (N-SI-009)	59
RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (N-SI-010)	64
TERMO DE USO DOS SISTEMAS DE INFORMAÇÃO (T-SI-001)	69



APRESENTAÇÃO

No contexto da informática, informação é o conjunto de dados coletados, transformados, armazenados e transmitidos por um sistema de processamento eletrônico de dados, ou seja, por computadores.

Por sua vez, dados e informações geram conhecimento, e este é o bem mais valioso de qualquer instituição. Além disso, os dados e informações processados pelo IpeM-SP dizem respeito a milhares de empresas e de cidadãos. Garantir o sigilo e a segurança desses dados é dever de todos os que trabalham no Instituto.

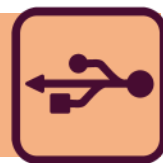
Este manual, baseado integralmente na “Política de Segurança da Informação do IpeM-SP” delineada na Portaria IpeM-SP nº 148/2020, contém diretrizes para orientar todos os colaboradores sobre as ações que visam proteger a informação.

Ações de proteção à informação devem ser ativamente buscadas, em particular por todos aqueles envolvidos com as atividades de tecnologia da informação, sejam servidores de carreira, contratados ou terceirizados, bem como empresas fornecedoras ou prestadoras de serviço na área de TI.

Assim, a leitura atenta deste manual é fundamental para que cada colaborador conheça e se comprometa com a aplicação das diretrizes aqui formuladas e se torne efetivamente engajado na segurança da informação.

Ronaldo de Oliveira e Silva

Diretor do Departamento de Tecnologia da Informação



PORTARIA IPEM-SP Nº 148 DE 14 DE DEZEMBRO DE 2020

O SUPERINTENDENTE DO INSTITUTO DE PESOS E MEDIDAS DO ESTADO DE SÃO PAULO – IPEM/SP, autarquia estadual, designado por meio do Decreto de 16 de janeiro de 2019, publicado no Diário Oficial do Estado em 17 de janeiro de 2019, de lavra do Governador do Estado de São Paulo, no desempenho de suas atribuições legais, consignadas na Lei n.º 9.286/1995 e Decreto n.º 55.964/2010;

Considerando a necessidade de o IpeM-SP manter a integridade das informações essenciais ao exercício de suas competências e, inclusive, quando envolver informações que demandem a manutenção do sigilo funcional;

Considerando que as informações mencionadas, ressalvados os direitos autorais, integram o patrimônio do IpeM-SP e devem ser protegidas;

Considerando que os diversos meios de suporte, a veiculação e o armazenamento da informação são vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, eventuais extravios e furtos, dentre outros;

Considerando a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas NBR ISO/IEC 27001:2013, NBR ISO/IEC 27002:2013, NBR ISO/IEC 27005:2011, às quais a Política Geral de Segurança da Informação (PGSI) do IpeM-SP deverá estar alinhada;

Considerando o Memorando DTIN n.º 010/2020, que apresenta a Política Geral de Segurança de Segurança da Informação (PGSI) e solicita a aprovação nos termos descritos naquele expediente (fls. 03/04);

Considerando a Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal e aprova a Estrutura de Gestão da Segurança da Informação dos órgãos e nas entidades da administração pública federal;

Considerando a emissão do Parecer IPEM/AGANP/FGPC n.º 229/2020 (fls. 45/48) ratificado pelo Diretor do Departamento de Recursos Humanos e Apoio Jurídico (fl. 48), que opinam pela implementação da Política Geral de Segurança da Informação (PGSI), no âmbito interno do IpeM-SP;

RESOLVE:



Portaria Ipem-SP nº 148/2020

Artigo 1º - ESTABELECE A POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO (PGSI) no Ipem-SP, como parte do sistema de gestão institucional baseada em normas e boas práticas com o objetivo de efetivar diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação no âmbito interno desta autarquia, nos termos da Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a estrutura de gestão de segurança da informação nos órgãos e nas entidades da administração pública federal, conforme os itens que seguem:

- I – Política Geral de Segurança da Informação – código: P-SI-001;
- II – Classificação, Rotulagem e Manuseio da Informação – código: N-SI-001;
- III – Uso Aceitável de Ativos de Informação – código: N-SI-002;
- IV – Norma de Gestão de Identidade e Controle de Acesso – código: N-SI-003;
- V – Norma de Acesso à Internet e Comportamento em Mídias Sociais – código: N-SI-004;
- VI – Norma de Uso de Serviços de E-mail e Comunicadores Instantâneos – código: N-SI-005;
- VII – Norma de Proteção Contra Códigos Maliciosos – código: N-SI-006;
- VIII – Norma de Uso de Equipamentos Computacionais Pessoais – código: N-SI-007;
- IX – Norma de Acesso Remoto – código: N-SI-008;
- X – Norma de Monitoramento de Ativos e Serviços da Informação – código: N-SI-009;
- XI – Norma de Resposta a Incidentes de Segurança da Informação – código N-SI-010;
- XII – Termo de Uso dos Sistemas de Informação – código: T-SI-001.

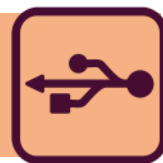
Artigo 2º - Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

PUBLIQUE-SE, REGISTRE-SE E CUMPRA-SE.

São Paulo, 14 de dezembro de 2020.

RICARDO GAMBARONI

Superintendente



POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

Texto redigido com base na NORMA P-SI-001

Introdução

O Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP é uma autarquia vinculada à Secretaria da Justiça e Cidadania do Governo do Estado de São Paulo e órgão delegado do Inmetro. Tem como missão executar as atividades metrológicas e da avaliação da conformidade alicerçadas na rastreabilidade de seus padrões, buscando inovação e executando serviços essenciais na proteção ao cidadão em suas relações de consumo exercendo, no âmbito do Estado, a verificação e a fiscalização de:

- instrumentos de medição (e medidas materializadas) sujeitos à metrologia legal;
- produtos pré-medidos;
- produtos têxteis;
- produtos com certificação compulsória;
- veículos transportadores de produtos perigosos e de GLP fracionado.

O Ipem-SP dispõe também de um Centro Tecnológico para prestar serviços de calibração de padrões metrológicos e instrumentos de medição.

O Ipem-SP entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados à sociedade.



Política Geral de Segurança da Informação

O Ipem-SP compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

Dessa forma, o Ipem-SP estabelece sua Política Geral de Segurança da Informação (PGSI), como parte integrante do seu sistema de Governança Corporativa, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da instituição ou sob sua responsabilidade.

Propósito

Esta política, tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores do Ipem-SP adotar padrões de comportamento seguro, adequados às metas e necessidades do próprio Instituto;

Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

Resguardar as informações do Ipem-SP, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes, fiscalizados ou cidadãos em geral ou de qualquer outro impacto negativo nas atividades do Ipem-SP como resultado de falhas de segurança.



Política Geral de Segurança da Informação

Escopo

Esta política se aplica a todos os usuários da informação do Ipem-SP, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o Ipem-SP, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores e visitantes que possuam, possuem ou virão a possuir acesso às informações do Ipem-SP e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do Ipem-SP.

Diretrizes

O objetivo da gestão de Segurança da Informação do Ipem-SP é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas das suas atividades e minimizando riscos identificados e seus eventuais impactos à instituição.

A Superintendência, Diretoria Executiva e o Comitê Gestor de Segurança da Informação - CGSI estão comprometidos com uma gestão efetiva de Segurança da Informação no Ipem-SP. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas pelo CGSI para garantir sua contínua pertinência e adequação às necessidades do Ipem-SP.

É política do Ipem-SP:

Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do Ipem-SP sejam



Política Geral de Segurança da Informação

atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: empregados, terceiros contratados, fornecedores, visitantes e, onde pertinente, clientes.

Garantir a educação e conscientização sobre as práticas adotadas pelo IPEM-SP de segurança da informação para empregados, terceiros contratados, fornecedores, visitantes e, onde pertinente, clientes.

Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

Tratar integralmente incidentes de segurança da informação, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

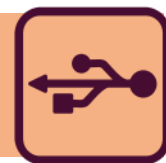
Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

Papéis e Responsabilidades

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI

Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, formado pelo Diretor do Departamento de Tecnologia da Informação (DTIN), designado como Presidente do Comitê, e um representante de cada uma das seguintes áreas: Superintendência, área de Recursos Humanos, área Jurídica e



Política Geral de Segurança da Informação

área de Comunicação social. É responsabilidade do CGSI:

Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do IpeM-SP.

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO - GSI

Fica constituída a Gerência de Segurança da Informação, sistematizada pela Diretoria de Infraestrutura – TINTI pertencente ao Departamento de Tecnologia da Informação – DTIN.

É responsabilidade da Gerência de Segurança da Informação:

Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI; Apoiar o CGSI em suas deliberações; Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para fazer cumprir a PGSI;

Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovadas, implantar medidas corretivas para reduzir o risco e tomar ações cabíveis para fazer cumprir os termos desta política;

Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.



Política Geral de Segurança da Informação

GESTORES DA INFORMAÇÃO

É responsabilidade dos Gestores da Informação em de cada departamento:

Gerenciar as informações geradas ou sob a responsabilidade da sua área durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo Ipem-SP;

Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área conforme normas, critérios e procedimentos adotados pelo Ipem-SP;

Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área, ajustando a classificação e rotulagem conforme necessário;

Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

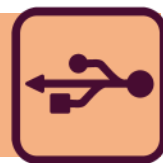
Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo Ipem-SP.

USUÁRIOS DA INFORMAÇÃO

É responsabilidade dos Usuários da Informação:

Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos à Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;



Política Geral de Segurança da Informação

Comunicar à Gerência de Segurança da Informação através de registro de incidente na Central de Serviços qualquer evento que viole esta Política e coloque, ou possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do Ipem-SP;

Assinar o Termo de Uso de Sistemas de Informação do Ipem-SP, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

A aplicação de sanções e punições será realizada mediante processo formal conforme a análise e parecer do Comitê Gestor de Segurança da Informação o qual deverá considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, sugerir a pena que entender cabível quando tipificada a falta grave;

No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;



Política Geral de Segurança da Informação

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao Ipem-SP, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos parágrafos acima.

Casos Omissos

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

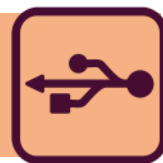
As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança da informação, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do Ipem-SP adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do Ipem.

Glossário

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar o Ipem;

Ativo: Tudo aquilo que possui valor para o Ipem-SP;

Ativo de informação: Patrimônio intangível do Ipem-SP, constituído por informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao Ipem-SP por parceiros, clientes, fiscalizados, cidadãos, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do Ipem-SP ou por infraestrutura externa contrata-



Política Geral de Segurança da Informação

da pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Comitê Gestor de Segurança da Informação—CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do Ipem-SP, que tem por finalidade tratar questões ligadas à Segurança da Informação.

Confidencialidade: Propriedade dos ativos da informação do Ipem-SP, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pelo Ipem-SP para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação do Ipem-SP, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do Ipem-SP.

Integridade: Propriedade dos ativos da informação do Ipem-SP, de serem exatos e completos.

Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação do Ipem-SP.

Segurança da informação: A preservação das propriedades de confidenciali-



Política Geral de Segurança da Informação

dade, integridade e disponibilidade das informações do Ipem-SP.

Usuário da informação: Empregados com vínculo empregatício de qualquer área do Ipem-SP ou terceiros alocados na prestação de serviços no Ipem-SP, indiferentemente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do Ipem-SP para o desempenho de suas atividades profissionais.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do Ipem-SP.

Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Política

A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



CLASSIFICAÇÃO, ROTULAGEM E MANUSEIO DA INFORMAÇÃO

Texto redigido com base na NORMA N-SI-001

Introdução

A Norma de segurança da informação N-SI-001 complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para a classificação, rotulagem, manuseio, guarda e descarte seguro de informações em formato digital ou em suporte físico.

Propósito

Estabelecer diretrizes para a classificação, manuseio e rotulagem dos ativos de informação do Instituto de Pesos e Medidas – Ipem-SP por seus usuários autorizados.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Classificação e rotulagem da Informação

Para efeitos de classificação da informação, o Ipem-SP utiliza as seguintes categorias:



Classificação, rotulagem e manuseio da Informação

INFORMAÇÃO PÚBLICA: Informação oficialmente liberada pelo Ipem-SP para o público geral. A divulgação deste tipo de informação não causa problemas ao Ipem-SP ou a seus clientes, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.

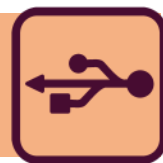
INFORMAÇÃO DE USO INTERNO: Informação liberada exclusivamente para usuários e departamentos específicos do Ipem-SP, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização expressa.

INFORMAÇÃO CONFIDENCIAL: Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais no Ipem-SP. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para o Ipem-SP e/ou seus clientes, portanto seu compartilhamento deve ser restrito e feito de maneira controlada.

A classificação da informação deverá ser realizada pelos gestores da informação, ou colaboradores designados por estes. Entretanto, a responsabilidade pela assertividade do nível selecionado permanece com o gestor da informação;

Para informações classificadas como PÚBLICAS, poderá ser utilizada um rótulo simples, conforme modelos exibidos no Anexo I desta norma;

Para informações classificadas como USO INTERNO ou CONFIDENCIAIS, deverá constar no rótulo a sua classificação e, quando o acesso à informação for limitado a um setor/departamento específico, o mesmo deverá ser referenciado, conforme modelos exibidos no Anexo I desta norma;



Classificação, rotulagem e manuseio da Informação

Para a rotulagem da informação, devem ser observados os modelos contidos no Anexo I desta norma.

Manuseio da Informação

O manuseio da informação do IpeM deverá obedecer às regras definidas na Tabela Ação x Classificação, detalhada no Anexo II desta norma;

Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas;

Em períodos de ausência da estação de trabalho, documentos em suporte físico devem ser retirados das mesas e de outras áreas de superfície;

Documentos de uso interno ou confidenciais em suporte eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas;

Toda não-conformidade será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação (PGSI), conforme a gravidade da violação.

Descarte da Informação

O descarte da informação deve ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original;

O descarte da informação deverá ser realizado conforme os métodos estabelecidos no Anexo III desta norma.

Papéis e Responsabilidades



Classificação, rotulagem e manuseio da Informação

GESTOR DA INFORMAÇÃO

É responsabilidade do colaborador apontado como Gestor da Informação:

Definir a classificação das informações sob sua responsabilidade com base nas categorias de classificação constantes desta norma, mantendo um registro atualizado dos itens classificados;

Controlar as informações geradas em sua área de negócio e atuação;

Revisar periodicamente a classificação das informações sob sua guarda.

Sanções e Punições

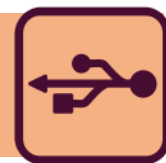
Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma N-SI-001 é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência da Ipem.





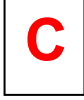
Classificação, rotulagem e manuseio da Informação

ANEXO I

MODELOS PARA ROTULAGEM DE INFORMAÇÕES

Os padrões a seguir representam os rótulos aprovados que devem ser exibidos nos cabeçalhos e rodapés de documentos de acordo com seu nível de classificação.

Observação: A cor, fonte e tamanho do texto podem ser ajustados para adequação a informação rotulada, desde que mantida a clareza e objetividade da informação.

Nível	Rótulo
Informação Pública (Rotulagem opcional)	 <i>Informação Pública</i> <i>Public Information</i>
Informação Interna	 <i>Informação Interna</i> <i>Internal Information</i>
Informação Confidencial	 <i>Informação Confidencial</i> <i>Confidential Information</i>

Cabeçalho

Rodapé

Ipem – [INSERIR NÍVEL DE CLASSIFICAÇÃO/SETOR] .

Exemplo:

Ipem – Uso Interno / Departamento de Recursos Humanos

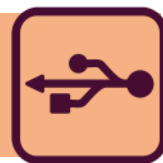


Classificação, rotulagem e manuseio da Informação

ANEXO II

TABELA AÇÃO X CLASSIFICAÇÃO

AÇÃO	CLASSIFICAÇÃO		
	Pública	Interna	Restrita / Confidencial
Cópia / Exclusão	Sem restrições	Sem restrições	Permissão do gestor da informação
Envio por Fax	Sem restrições	Usar folha de rosto padronizada	Usar folha de rosto padronizada
Transmissão em rede pública	Permitido	Permitido	Recomendável Comunicação criptografada.
Descarte	Lixo comum	Lixo comum. Recomendável uso de fragmentadora.	Utilizar métodos aprovados conforme anexo desta norma.
Envio a terceiros	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação e termo de confidencialidade assinado pelo terceiro.
Solicitação de direitos de acesso	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação
Correio interno e externo	Envelope comum	Envelope comum	Envio para destinatário específico identificado apenas dentro do envelope.
Rotulagem	Opcional	Na capa e em todas as páginas	Na capa e em todas as páginas.
Registro de Acompanhamento	Opcional	Opcional	Destinatários, cópias efetuadas, localização e endereço de todos que acessaram e destruição.



Classificação, rotulagem e manuseio da Informação

ANEXO III

MÉTODOS DE DESCARTE PARA INFORMAÇÕES ARMAZENADAS ELETRONICAMENTE

Os métodos a seguir foram selecionados como forma segura de garantir o descarte de informações do IpeM-SP. Para todos os métodos que envolvem atividades técnicas, os usuários deverão encaminhar a solicitação para a área de tecnologia da informação.

Método	Descrição	Aplicável a
Sobre gravar mídia	Sobre gravar dados em mídias de armazenamento magnético com informações não sensíveis por pelo menos 07 vezes. Essa tarefa pode ser executada com o auxílio de software/hardware especializado. Este método não destrói fisicamente a mídia, entretanto destrói todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis, CDR, DVDR e similares;
Destruição física	Destruição física da mídia de armazenamento com o uso de picotadores especializados, pulverizadores ou incineradores. Este método destrói completamente a mídia e todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis. CD, CDR, DVD, DVDR. Este método também é válido para material em suporte físico como impressos e similares;
Desmagnetização	Desmagnetização de mídias como fitas e disquetes. Este método destrói todos os dados.	Fitas e disquetes.
Criptografia de caminho único (One-Way)	Uso de um hash do tipo one-way para criptografar a informação de forma irrecuperável, mesmo que de posse da chave de criptografia. Recomenda-se o uso do hash SHA256. Este método não afeta a mídia e pode ser usado para o descarte seletivo de informações.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis, CDR, DVDR e similares;



USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO

Texto redigido com base na NORMA N-SI-002

Introdução

A Norma de segurança da informação **N-SI-002** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para o uso aceitável de ativos de informação do Ipem-SP por seus usuários autorizados.

Propósito

Estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação do Instituto de Pesos e Medidas – Ipem-SP por seus usuários autorizados.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Uso de equipamento computacional

O Ipem-SP fornece para seus usuários equipamentos para o desempenho **exclusivo** de suas atividades profissionais. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do Ipem-SP:



Uso aceitável de ativos de Informação

Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do Ipem-SP, sendo expressamente proibida a utilização para fins particulares;

A alteração e/ou a manutenção de qualquer equipamento de propriedade do Ipem-SP é uma atribuição específica do Departamento de Tecnologia da Informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

Os equipamentos do Ipem-SP devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

Computadores de mesa (*desktops*) ou móveis (*notebooks ou tablets*) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

A desconexão (*log off*) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com o Ipem-SP; e

Qualquer dano aos equipamentos do Ipem-SP será devidamente analisado



Uso aceitável de ativos de Informação

pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu da ação direta ou omissão do usuário, caberá ao Ipem-SP exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.

A seu critério exclusivo, o Ipem-SP poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo passar por inspeção pelo Departamento de Tecnologia da Informação, de forma a garantir adequação aos requisitos e controles de segurança adotados pelo Ipem-SP;

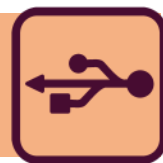
Não é permitida a conexão de equipamentos particulares na rede administrativa do Ipem-SP, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento pelo Departamento de Tecnologia da Informação.

Dispositivos de Armazenamento Removível

O Ipem-SP poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes:

O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, não deverão ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos;



Uso aceitável de ativos de Informação

A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de tecnologia da informação e é obrigatória para todos os equipamentos corporativos; e

Em caso de perda ou furto de um dispositivo móvel, o usuário deve providenciar um registro na Central de Serviços (Helpdesk) e comunicar imediatamente seu superior imediato para que possam ser tomadas as medidas cabíveis.

Armazenamento remoto (nuvem)

O IpeM-SP disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa;

A responsabilidade pelos dados e informações armazenadas nesse local é do próprio usuário;

Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela instituição e homologada pela equipe de segurança da informação do IpeM-SP.

Identificação digital

O IpeM-SP poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que executem atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:

Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

O usuário deverá informar a equipe de segurança da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;



Uso aceitável de ativos de Informação

O usuário desligado ou em processo de desligamento terá o certificado digital expedido pelo Ipem-SP imediatamente revogado;

É responsabilidade da área de segurança da informação prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.

Equipamentos de impressão e reprografia

O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do Ipem ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:

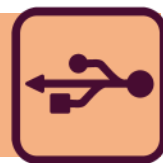
O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos de que tenha solicitado a impressão, transmissão ou cópia que contenham informações do Ipem-SP, classificadas como de uso interno ou confidencial;

A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo serem descartadas de acordo com os procedimentos adotados pelo Ipem-SP.

Segurança física

As instalações de processamento das informações do Ipem-SP são consideradas áreas sensíveis e serão mantidas seguras, com perímetro fisicamente iso-



Uso aceitável de ativos de Informação

lado contra acesso não autorizado, contra danos e quaisquer interferências de origem humana ou natural. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que não são colaboradores do Ipem-SP;

Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis do Ipem-SP;

É resguardado ao Ipem-SP o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;

É resguardado ao Ipem o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;

Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas. Assim, ao se ausentar, cabe ao usuário o dever de mantê-los guardados, ou descartá-los de



Uso aceitável de ativos de Informação

acordo com os procedimentos determinados pelo Ipem-SP;

Não é permitido consumir qualquer tipo de alimento ou bebida ou nas áreas apontadas como sensíveis.

Papéis e Responsabilidades

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade da Gerência de Segurança da Informação:

Estabelecer e manter atualizados os procedimentos complementares a esta norma;

Comunicar ao CGSI eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.

Sanções e Punições

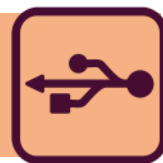
Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-002** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem.



GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO

Texto redigido com base na NORMA N-SI-003

Introdução

A Norma de segurança da informação **N-SI-003** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação do Instituto de Pesos e Medidas - Ipem-SP garanta níveis adequados de proteção.

Propósito

Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação do Ipem-SP.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Acesso a ativos e sistemas de informação

O Ipem-SP fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;



Gestão de identidade e controle de acesso

As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

Toda conta de acesso é pessoal do usuário a qual foi delegada, e é intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo Ipem-SP;

Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo Ipem-SP;

Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;

Informar imediatamente a Central de Serviços caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do Ipem-SP;

Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos e serviços de informação ou recur-



Gestão de identidade e controle de acesso

os computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

Senha de acesso

As senhas associadas às contas de acesso a ativos e serviços de informação ou recursos computacionais do IpeM-SP são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

O IpeM-SP adota os seguintes padrões para geração de senhas de acesso a seus ativos e serviços de informação ou recursos computacionais:

A Central de Serviços (Helpdesk) será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder à troca imediata da mesma;

As senhas possuem validade de 180 (cento e oitenta) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;

As senhas serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais; Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo por, no mínimo, 30 (trinta) minutos; Os sistemas de informação manterão um histórico das últimas 3 (três) senhas utilizadas, não permitindo sua reutilização;

Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da Central de Serviços (Helpdesk).



Gestão de identidade e controle de acesso

Ao criar uma senha os usuários devem estar atentos às seguintes **recomendações**:

Não utilizar nenhuma parte da sua credencial na composição da senha;

Não utilizar qualquer um dos seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

Não utilizar repetição ou sequência de caracteres, números ou letras;

Qualquer parte ou variação do nome “Ipem-SP”;

Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

Autorização de acesso (privilégios de acesso)

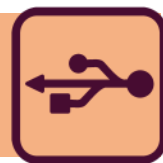
A autorização e o nível permitido de acesso aos ativos e serviços de informação do Ipem-SP é feita com base em perfis que definem o nível de privilégio dos usuários.

O acesso aos ativos e serviços de informação é fornecido a critério do Ipem-SP, que define permissões baseadas nas necessidades laborais dos usuários;

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas à Central de Serviços.

Os usuários devem ainda observar as seguintes diretrizes:

A seu critério exclusivo, o Ipem-SP poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local, ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço,



Gestão de identidade e controle de acesso

deverá fazer uma solicitação à Central de Serviços (Helpdesk).

É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse do Ipem-SP, seja na infraestrutura computacional local ou nos serviços de armazenamento remoto (nuvem);

Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) do Ipem-SP.

Papéis e Responsabilidades

GESTOR DA INFORMAÇÃO

É responsabilidade do colaborador apontado como Gestor da Informação:

Autorizar a concessão e revogação de acesso a ativos e sistemas de informação sob sua responsabilidade;

Autorizar a concessão e o controle de acesso administrativo a ativos e sistemas de informação sob sua responsabilidade;

Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos e sistemas de informação sob sua responsabilidade.

DEPARTAMENTO DE RECURSOS HUMANOS

É responsabilidade do departamento DE Recursos Humanos:

Reportar em tempo hábil o desligamento de empregados do Ipem-SP à Central de Serviços (Helpdesk) para que contas de acesso possam ser revogadas;

Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posto ou lotação no Ipem-SP;



Gestão de identidade e controle de acesso

Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

GESTORES E COORDENADORES

É responsabilidade dos gestores e coordenadores:

Solicitar à Central de Serviços (Helpdesk) a concessão de acesso a novos empregados, ou empregados que necessitem de novos acessos, conforme mudanças em suas atividades laborais;

Solicitar à Central de Serviços (Helpdesk) a concessão de acesso a terceiros e prestadores de serviços contratados, justificando a necessidade do acesso a ativos e sistemas de informação;

Informar à Central de Serviços (Helpdesk) quando do encerramento do contrato com terceiros e prestadores de serviços contratados que tenham acesso a ativos e sistemas de informação.

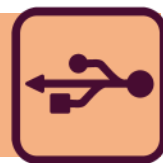
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade do Departamento de Tecnologia da Informação por intermédio da Central de Serviços (Helpdesk) :

Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários empregados, terceiros e prestadores de serviços;

Conceder, quando autorizado, o acesso aos usuários empregados, terceiros e prestadores de serviço, conforme indicado pelos gestores da informação;

Revogar, quando solicitado, o acesso dos usuários empregados, terceiros e prestadores de serviço, conforme indicado pelos gestores da informação;



Gestão de identidade e controle de acesso

Apoiar a revisão periódica da validade de credenciais de acesso a ativos e sistemas de informação dos usuários empregados, terceiros e prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos e sistemas de informação.

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-003** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS

Texto redigido com base na NORMA N-SI-004

Introdução

A Norma de segurança da informação **N-SI-004** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para utilização segura do acesso à internet fornecido pelo Instituto de Pesos e Medidas – Ipem-SP e do comportamento de colaboradores em mídias e redes sociais.

Propósito

Estabelecer diretrizes para utilização segura do acesso à internet fornecido pelo Instituto de Pesos e Medidas – Ipem-SP e do comportamento de colaboradores em mídias e redes sociais.

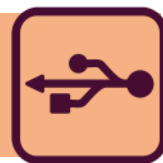
Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Acesso à internet

O Ipem-SP fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;



Acesso à internet e comportamento em mídias sociais

O acesso à internet pode ser fornecido tanto através da rede corporativa do Ipem, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pelo Ipem-SP;

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pelo Ipem-SP está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

Durante o monitoramento do acesso à internet, o Ipem-SP se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;

Durante o acesso à Internet fornecido pelo Ipem-SP não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:

Qualquer espécie de exploração sexual; qualquer forma de conteúdo adulto, erotismo, pornografia; qualquer tipo de pornografia infantil; qualquer forma de ameaça, chantagem e assédio moral ou sexual;

Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;



Acesso à internet e comportamento em mídias sociais

A prática e/ou a incitação de crimes ou contravenções penais; a prática de propaganda política nacional ou internacional; a prática de quaisquer atividades comerciais desleais; o desrespeito a imagem ou aos direitos de propriedade intelectual e industrial do Ipem-SP; a disseminação de códigos maliciosos e ameaças virtuais; a tentativa de expor a infraestrutura computacional do Ipem-SP a ameaças virtuais; a divulgação não autorizada de qualquer informação do Ipem-SP classificada como confidencial ou de uso interno; o uso de sites ou serviços que busquem contornar controles de acesso à internet.

Comportamento corporativo em mídias ou redes sociais

A publicação de conteúdo referente ao Ipem-SP em mídias ou redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da instituição;

Quando no uso de suas mídias ou redes sociais particulares, empregados, prestadores de serviço, terceiros contratados e visitantes devem observar as seguintes restrições:

Não é permitido o uso do logotipo, bem como de qualquer parte da identidade visual do Ipem-SP sem autorização prévia e expressa;

Não é permitida a criação, participação ou interação com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos do Ipem-SP, excetuando-se os canais oficiais da instituição;

Não é permitida a publicação de conteúdo ou comentários diretamente relacionados ao Ipem-SP;



Acesso à internet e comportamento em mídias sociais

Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo do Ipem-SP sem a expressa autorização da instituição, excetuando-se material divulgado em canais oficiais.

Papéis e Responsabilidades

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade do departamento de tecnologia da informação:

Controlar e monitorar qualquer tipo de acesso à internet fornecido pelo Ipem-SP;

Reportar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso à internet para a equipe de segurança da informação e ao CGSI.

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-004** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS

Texto redigido com base na NORMA N-SI-005

Introdução

A Norma de segurança da informação **N-SI-005** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos fornecidos pelo Instituto de Pesos e Medidas –Ipem-SP.

Propósito

Estabelecer diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pelo Instituto de Pesos e Medidas –Ipem-SP.

Escopo

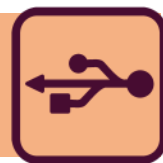
Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Serviço de E-Mail

O Ipem-SP fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

Não é permitido o uso de qualquer serviço de e-mail que não seja o oficialmente fornecido pelo Ipem-SP, exceto quando expressamente autorizado;



Uso de serviços de e-mail e comunicadores instantâneos

Quando o usuário fizer uso do serviço de e-mail do IpeM-SP, não é permitido:

Utilizar-se do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do IpeM-SP;

Utilizar-se de termos ou palavras de baixo calão na redação de mensagens;

Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do IpeM-SP, excetuando-se quando expressamente autorizados;

Inscriver o endereço de e-mail do IpeM-SP em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da instituição;

Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação (CGSI);

Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;

Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor; e usar o serviço de e-mail para o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;



Uso de serviços de e-mail e comunicadores instantâneos

O serviço de e-mail do Ipem-SP é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;

O monitoramento do serviço de e-mail do Ipem-SP tem como objetivos proteger a instituição, atestar o respeito às regras contidas nesta norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;

Durante o monitoramento, o Ipem-SP se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail;

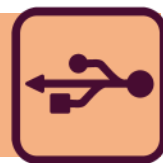
O Ipem adota um padrão para criação dos endereços de e-mail sendo composto pelas letras iniciais de cada nome, seguido do último sobrenome, conforme exemplo a seguir:

Nome completo do empregado: Isabela Antonini Soares Dodt;

E-mail: iasdodt@lpem.sp.gov.br.

Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão adotado pelo Ipem-SP. Não é permitido o uso de sobrenomes de filiação na composição do endereço de e-mail como, por exemplo, Junior, Filho, Neto, Segundo, Terceiro.

Os usuários do serviço de e-mail do Ipem-SP devem adotar a assinatura padrão, formatada de acordo com o modelo determinado pelo Governo do Estado de São Paulo.



Uso de serviços de e-mail e comunicadores instantâneos

Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:

“Esta mensagem, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar, copiar o seu conteúdo.”

Serviços de Comunicadores Instantâneos

O Ipem-SP fornece o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não seja o oficialmente fornecido pelo Ipem-SP, excetuando-se quando expressamente autorizado;

Quando o usuário fizer uso do serviço de comunicadores instantâneos do Ipem-SP, não é permitido:

Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de interesse do Ipem;

Utilizar de termos ou palavras de baixo calão na redação de mensagens;

Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para pessoas ou entidades que não fazem parte do domínio corporativo do Ipem-SP, excetuando-se quando expressamente autorizados;

Fazer uso de qualquer técnica forja ou simulação de falsa identidade. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de



Uso de serviços de e-mail e comunicadores instantâneos

segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;

A interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (SPAM) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de comunicadores instantâneos;

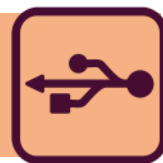
Usar o serviço de comunicadores instantâneos para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, não sendo permitido o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

O serviço de comunicadores instantâneos do IpeM-SP é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;

O monitoramento do serviço de comunicadores instantâneos do IpeM-SP tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;

Durante o monitoramento, o IpeM-SP se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, bloquear, redirecionar, re-



Uso de serviços de e-mail e comunicadores instantâneos

transmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de comunicadores instantâneos.

Papéis e Responsabilidades

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade do Departamento de Tecnologia da Informação:

Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pelo Ipem-SP;

Reportar eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao uso dos serviços de e-mail e comunicadores instantâneos para a equipe de segurança da informação e ao CGSI.

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-005** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Texto redigido com base na NORMA N-SI-006

Introdução

A Norma de segurança da informação **N-SI-006** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para proteção dos ativos e serviços de informação do Instituto de Pesos e Medidas – Ipem-SP contra ameaças e códigos maliciosos de qualquer natureza.

Propósito

Estabelecer diretrizes para a proteção dos ativos e serviços de informação do Instituto de Pesos e Medidas – Ipem-SP contra ameaças e códigos maliciosos de qualquer natureza.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Ferramenta de proteção contra códigos maliciosos

O Ipem-SP disponibiliza ferramentas para proteção dos seus ativos e serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos mali-



Proteção contra códigos maliciosos

ciosos tais como vírus, cavalos de troia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;

Apenas a ferramenta disponibilizada pelo Ipem-SP deve ser utilizada na proteção contra códigos maliciosos;

A ferramenta de proteção contra códigos maliciosos do Ipem-SP adota as seguintes regras de uso:

Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e proteção em estações de usuários e servidores corporativos;

As varreduras serão efetuadas quando necessário e devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;

As varreduras serão efetuadas quando necessário em servidores corporativos e podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;

Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;

Caso uma estação de usuário ou dispositivo móvel esteja infectada ou com suspeita de infecção de código malicioso, ela deverá ser imediatamente isolada da rede corporativa do Ipem-SP e de qualquer comunicação com a internet;



Proteção contra códigos maliciosos

Caso uma estação de trabalho esteja infectada ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o seu isolamento da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor.

Prevenção dos usuários contra códigos maliciosos

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários do Ipem-SP devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;

Os usuários do Ipem-SP devem seguir as seguintes regras para proteção contra códigos maliciosos:

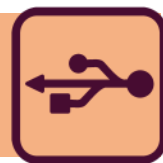
Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

Reportar imediatamente à Central de Serviços (Helpdesk) qualquer infecção ou suspeita de infecção por código malicioso;

Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;

Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pelo Ipem-SP antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;

Não habilitar ou executar macros, scripts ou arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da Central de Serviços para validar se o arquivo representa ou não uma ameaça.



Proteção contra códigos maliciosos

Papéis e Responsabilidades

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade do departamento de tecnologia da informação:

Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando os mesmos à equipe de segurança da informação e CGSI, caso necessário.

GERENCIA DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade da gerência de segurança da informação:

Garantir que novas modalidades de códigos maliciosos são adequadamente investigadas, tratadas e protegidas pela ferramenta corporativa adotada pelo Ipem-SP;

Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários do Ipem-SP.

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-006** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS

Texto redigido com base na NORMA N-SI-007

Introdução

A Norma de segurança da informação **N-SI-007** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do Instituto de Pesos e Medidas – Ipem - SP ou para o manuseio de informações do Ipem - SP.

Propósito

Estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do Ipem - SP ou para o manuseio de informações do Ipem - SP.

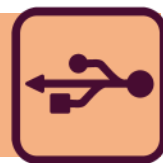
Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Uso de equipamentos computacionais pessoais no ambiente corporativo

O Ipem - SP fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;



Uso de equipamentos computacionais pessoais

A seu critério exclusivo, o Ipem - SP poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;

A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da Superintendência do Ipem - SP, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade do Ipem - SP;

O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política Geral de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções e punições previstas neste instrumento;

O Ipem - SP não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;

O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos do Ipem - SP não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas, permanecendo qualquer direito de propriedade intelectual com o Ipem - SP;

Quando autorizados a utilizar dispositivos de computação pessoal para execução de trabalho, de atividades ou manuseio de informações do Ipem - SP, os usuários serão inteiramente responsáveis por garantir a segurança dos seus



Uso de equipamentos computacionais pessoais

dispositivos, devendo garantir que o sistema operacional dos mesmos estará sempre atualizado e com todas as correções e melhorias de segurança aplicadas. Dispositivos de computação pessoal devem possuir ferramenta para prevenção de códigos maliciosos que garantam que as assinaturas de códigos maliciosos serão atualizadas em tempo real e executem varreduras quando necessário. Os dispositivos de computação pessoal devem utilizar apenas softwares licenciados, preservando o direito autoral.

Papéis e Responsabilidades

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)

É responsabilidade do CGSI:

Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo.

Sanções e Punições

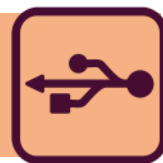
Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação (PGSI).

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-007** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do IpeM - SP.



ACESSO REMOTO

Texto redigido com base na NORMA N-SI-008

Introdução

A Norma de segurança da informação **N-SI-008** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para o acesso remoto a ativos e serviços de informação e recursos computacionais do Instituto de Pesos e Medidas – Ipem-SP.

Propósito

Estabelecer diretrizes para o acesso remoto a ativos e serviços de informação e recursos computacionais do Instituto de Pesos e Medidas – Ipem-SP, garantindo níveis adequados de proteção aos mesmos.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

Diretrizes

Concessão e uso do acesso remoto

O acesso remoto a ativos e serviços de informação e recursos computacionais do Ipem-SP é restrito aos usuários que necessitem deste recurso para execução das atividades profissionais;



Acesso remoto

A realização do acesso remoto, fora do expediente normal de trabalho, não implicará no pagamento de horas extras ao usuário, excetuando-se casos em que for comprovada a solicitação do trabalho pelo gestor do usuário ou parte autorizada;

O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros de posse de suas credenciais de acesso remoto;

O acesso remoto a ativos e serviços de informação e recursos computacionais do Ipem-SP será concedido ao usuário com os privilégios mínimos necessários para execução de suas atividades laborais;

Equipamentos computacionais pessoais do usuário utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do Ipem-SP e firewall local ativo;

Em casos de acesso não autorizado, extravio, mau uso, furto ou roubo de dispositivos computacionais, corporativos ou pessoais que possuam o acesso remoto ao ambiente do Ipem-SP habilitado, o usuário responsável deverá informar imediatamente o ocorrido à Central de Serviços (Helpdesk) do Ipem-SP.

Concessão e uso do acesso remoto para terceiros

O acesso remoto a ativos e serviços de informação e recursos computacionais do Ipem-SP poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais;

Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:

O acesso remoto de terceiros e prestadores de serviço a ativos e serviços de



Acesso remoto

informação ou recursos computacionais do Ipem-SP somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes;

A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado para a atividade do terceiro ou prestador de serviço, não excedendo o máximo de 30 (trinta) dias corridos por concessão;

O usuário terceiro, bem como a empresa onde trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais de acesso remoto;

O acesso remoto de terceiros a ativos e serviços de informação e recursos computacionais do Ipem-SP será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do Ipem-SP e firewall local ativo;

Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possuam o acesso remoto ao ambiente do Ipem-SP habilitado, o usuário responsável deverá informar imediatamente o ocorrido a Central de Serviços (Helpdesk) do Ipem-SP.

Monitoramento do acesso remoto

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos e serviços de informação ou recursos computacionais do Ipem-SP está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;



Acesso remoto

Durante o monitoramento do acesso remoto a seus ativos e serviços de informação ou recursos computacionais, o Ipem-SP se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

Papéis e Responsabilidades

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade da gerência de segurança da informação:

Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos e serviços de informação ou recursos computacionais do Ipem-SP, e controlar e monitorar qualquer tipo de acesso remoto fornecido pelo Ipem-SP;

Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar ao CGSI.

Sanções e Punições

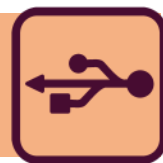
Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação (PGSI).

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-008** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem-SP.



MONITORAMENTO DE ATIVOS E SERVIÇOS DE INFORMAÇÃO

Texto redigido com base na NORMA N-SI-009

Introdução

A Norma de segurança da informação **N-SI-009** complementa Política Geral de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos e serviços de informação e recursos computacionais do Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP.

Propósito

Estabelecer diretrizes para o monitoramento de ativos e serviços de informação e recursos computacionais do Ipem-SP, garantindo o respeito dos usuários às regras estabelecidas na Política Geral de Segurança da Informação, bem como produzir prova de eventual violação das suas condições e na legislação vigente.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação (PGSI).

Diretrizes

Monitoramento de ativos serviços da informação e recursos computacionais



Monitoramento de ativos e serviços de informação

Qualquer ativo e serviço de informação ou recurso computacional do IpeM-SP, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento;

Todos os ativos e serviços de informação, recursos computacionais do IpeM-SP, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, estão sujeitos à monitoração, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança dos ativos de informação, bem como segurança jurídica do IpeM;

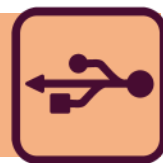
Não há expectativa de privacidade na utilização dos ativos e serviços de informação ou recursos computacionais do IpeM-SP, incluindo a utilização da conta de e-mail corporativa, comunicadores instantâneos e navegação em sites da Internet, através da infraestrutura tecnológica do IpeM;

Todas as informações dos ativos e serviços de informação ou recursos computacionais do IpeM-SP podem ser interceptadas, gravadas, lidas, copiadas e divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais. Estas informações incluem dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade.

Monitoramento do ambiente físico

O IpeM-SP faz o monitoramento do seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências;

As câmeras de filmagem estão dispostas de forma a resguardar a dignidade



Monitoramento de ativos e serviços de informação

humana, sendo vedada a sua instalação em banheiros, lavabos e na área reservada ao atendimento médico de empregados;

A filmagem descrita nesta norma tem por objetivo assegurar a segurança física do ambiente do Ipem-SP, bem como a sua segurança patrimonial, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, ficando o usuário ciente através deste item;

As imagens captadas dentro das dependências do Ipem-SP serão arquivadas conforme procedimento adotado pela instituição e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes em suas políticas e normas e/ou infração de legislação vigente;

O Ipem-SP não permite o uso de qualquer dispositivo de gravação audiovisual dentro do seu perímetro físico, excetuando-se quando o usuário estiver formalmente autorizado.

Aviso legal

O Ipem-SP faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso a ativos e serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas pelo Ipem-SP, bem como do monitoramento realizado nos termos desta norma.

O aviso legal deverá ser exibido antes de permitir o acesso a ativos e serviços de informação ou recursos computacionais do Ipem, apresentando o seguinte formato:

“Este é um ativo/serviço de informação ou recurso computacional do Ipem, o



Monitoramento de ativos e serviços de informação

qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste sistema, o infrator estará sujeito às sanções cabíveis nas esferas administrativa, cível e penal, sem prejuízo das demais legislações aplicáveis. Este ativo/serviço de informação ou recurso computacional é monitorado, não havendo expectativa de privacidade na sua utilização. O acesso a este ativo/serviço de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos.”

O acesso a qualquer ativo/serviço de informação ou recurso computacional do Ipem-SP ou o uso deles por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal;

A ausência do aviso legal em qualquer ativo/serviço de informação ou recurso computacional do Ipem-SP não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pelo Ipem-SP.

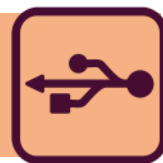
Papéis e Responsabilidades

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade do departamento de tecnologia da informação:

Realizar o monitoramento dos ativos e serviços de informação ou recursos computacionais do Ipem;

Tratar eventuais violações das diretrizes de segurança da informação do Ipem-SP identificadas através de ferramentas de monitoramento, e, quando pertinente, reportar as mesmas à equipe de segurança da informação e ao CGSI.



Monitoramento de ativos e serviços de informação

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Gestão da Norma

A norma **N-SI-009** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Superintendência do Ipem.



RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Texto redigido com base na NORMA N-SI-010

Introdução

A Norma de segurança da informação **N-SI-010** complementa Política Geral de Segurança da Informação (PGSI), definindo as diretrizes para responder eventos ou incidentes de segurança que estejam impactando ou possam vir a impactar ativos e serviços de informação ou recursos computacionais do Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP.

Propósito

Estabelecer as diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos e serviços de informação ou recursos computacionais do Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP.

Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação (PGSI).

Diretrizes

Incidentes de segurança da informação



Resposta a incidentes de segurança da informação

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos e serviços de informação ou recursos computacionais do Ipem serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

Incidentes de segurança devem ser priorizados com base na criticidade dos ativos e serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;

Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados à área de segurança da informação por intermédio de abertura de incidente na Central de Serviços (Helpdesk);

A área de segurança da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação;

Na ocorrência de um incidente de segurança da informação, ativos e serviços de informação ou recursos computacionais com suspeita de terem sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;

A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;



Resposta a incidentes de segurança da informação

Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

Time de resposta a incidentes de segurança da informação

O time de resposta a incidentes de segurança da informação do IpeM-SP deverá ser composto por, no mínimo, representantes das seguintes áreas:

Gerência de Tecnologia da Informação—DTIN

Gerência de segurança da informação - TINTI;

Gerência de recursos humanos;

Gerência jurídica.

Conforme a natureza do incidente, colaboradores de qualquer setor do IpeM-SP podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

Disseminação de informação sobre incidentes de segurança da informação

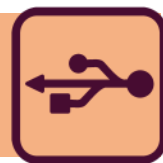
Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas ao IpeM-SP sem aprovação expressa e formal da Superintendência.

Papéis e Responsabilidades

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade da gerência de segurança da informação:

Atuar como responsável por ocorrências e eventos de segurança e garantir a



Resposta a incidentes de segurança da informação

existência de recursos para identificar, escalar, mitigar, conter e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos e serviços de informação ou recursos computacionais afetados pelo incidente;

Comunicar prontamente o time de resposta a incidentes de segurança da informação do Ipem-SP sobre eventos e incidentes de segurança.

TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade do time de resposta a incidentes de segurança da informação apoiar a equipe de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;

Aconselhar a superintendência do Ipem-SP sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.

COMUNICAÇÃO

É responsabilidade da assessoria de comunicação:

Providenciar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação (PGSI).



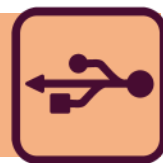
Resposta a incidentes de segurança da informação

Revisões

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação (CGSI).

Gestão da Norma

A norma **N-SI-010** é aprovada pelo Comitê Gestor de Segurança da Informação (CGSI), em conjunto com a Superintendência do Ipem-SP.



TERMO DE USO DE SISTEMAS DE INFORMAÇÃO

Texto redigido com base na NORMA T-SI-001

CONSIDERANDO que o Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP disponibiliza a seus usuários ativos de informação e recursos computacionais exclusivamente para que possam desempenhar suas atividades profissionais;

CONSIDERANDO que o Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP é o único proprietário de todos os ativos de informação e recursos computacionais, dessa forma, sendo responsável por todos os seus custos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

CONSIDERANDO que o Instituto de Pesos e Medidas do Estado de São Paulo – Ipem-SP poderá ser seriamente impactado pela indevida utilização de seus ativos de informação e recursos computacionais;

DECLARO QUE:

Tenho conhecimento e acesso à Política Geral de Segurança da Informação (PGSI), bem como às demais normas e procedimentos de Segurança da Informação necessárias ao meu trabalho, que se encontram disponíveis no portal corporativo do Ipem-SP, as quais li na íntegra, tomando conhecimento e ciência das suas disposições;



Termo de uso de sistemas de informação

Compreendi completamente os termos, diretrizes, conceitos e condições de uso da Política Geral de Segurança da Informação (PGSI), bem como as demais normas e procedimentos de Segurança da Informação necessárias ao meu trabalho, comprometendo-me a cumprir integralmente as disposições constantes em tais documentos;

Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica do Instituto de Pesos e Medidas do Estado de São Paulo – IpeM-SP somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades do instituto;

Estou ciente de que é realizado o monitoramento de todos os acessos, serviços e comunicações feitos através da infraestrutura tecnológica do Instituto de Pesos e Medidas do Estado de São Paulo – IpeM-SP;

Estou ciente de que as violações da Política Geral de Segurança da Informação (PGSI), bem como às demais normas e procedimentos de Segurança da Informação são passíveis de sanções e punições, e que posso incorrer em responsabilização legal nas esferas administrativa, cível e penal, nos termos da legislação em vigor caso as cometa;

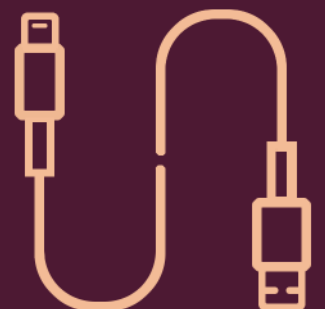
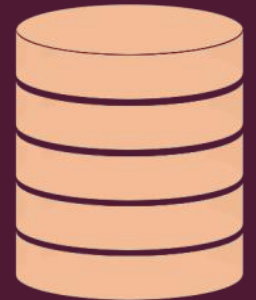
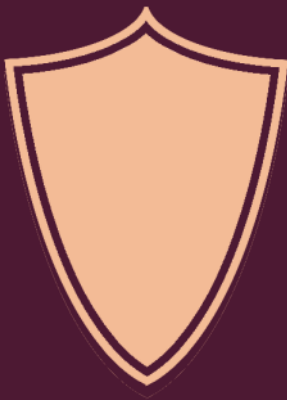
Comprometo-me a não revelar, fato, dado ou informações de qualquer natureza a que tenha conhecimento por força das minhas atribuições, que tenha contato ou acesso, mesmo após o encerramento do meu contrato de trabalho com o Instituto de Pesos e Medidas do Estado de São Paulo – IpeM-SP;

São Paulo, ____ de _____ de 20__.

Nome:

Cargo:

CPF:





IPEM 



TI



Secretaria da Justiça
e Cidadania



GOVERNO DO ESTADO
DE SÃO PAULO