Prefeitura de Joinville

Diário Oficial Eletrônico do Município de Joinville nº 1874
Disponibilização: 06/01/2022
Publicação: 06/01/2022

PORTARIA SEI - IPREVILLE.GAB/IPREVILLE.UJU

PORTARIA Nº 05, de 06 de janeiro de 2022.

Dispõe sobre a 3ª. Versão da Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville.

.

O Diretor-Presidente do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville - IPREVILLE, no uso da atribuição que lhe confere o artigo 112, alínea "j", da Lei Municipal nº 4.076, de 22 de dezembro de 1999, resolve:

Art. 1º Fica revisada a segunda versão da Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville (PSTI) para fins de instituir sua terceira versão.

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

Joinville, 06 de janeiro de 2022.

Guilherme Machado Casali
Diretor-Presidente do IPREVILLE

ANEXO I

P.S.T.I.

POLÍTICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO

INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE JOINVILLE

IPREVILLE

3ª VERSÃO – NOVEMBRO/2021

1. Apresentação

Este documento estabelece a PSTI – Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville – IPREVILLE, conjunto de diretrizes necessárias à preservação e segurança do Ambiente de Tecnologia da Informação do instituto.

São considerados pertencentes ao ambiente de TI – Tecnologia da Informação do IPREVILLE, os seguintes componentes/ativos: sistemas aplicativos desenvolvidos e adquiridos, softwares básicos e de apoio, dados, arquivos (virtuais/lógicos), hardware e equipamentos de infra-estrutura.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A segurança da tecnologia da informação, objetiva proteger o instituto de diversos tipos de ameaça, para garantir a continuidade do negócio, bem como, minimizar os danos.

A informação pode transitar de muitas formas, sendo possível armazená-la eletronicamente em dispositivos removíveis, transmiti-la pelo correio eletrônico ou através de outros meios eletrônicos. Seja qual for o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

A segurança da tecnologia da informação é aqui caracterizada pela preservação da:

- Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
- Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade, que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

A segurança da tecnologia da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, instruções de trabalho e funções de software. Estes controles precisam ser implementados para garantir que os objetivos de segurança específicos do IPREVILLE sejam atendidos.

Os riscos típicos que a PSTI do IPREVILLE pretende eliminar ou reduzir são:

- Revelação de informações sensíveis;
- Modificações indevidas de dados e programas;

- Perda de dados e programas;
- Destruição ou perda de recursos computacionais;
- Interdições ou interrupções de serviços essenciais;
- Roubo de propriedades.

Fica definido o termo "não-conformidade" como o evento apresentado pela infra-estrutura, hardware ou software, ou a ação ou atitude de quaisquer dos agentes citados por esta PSTI, que venham a comprometer a segurança da tecnologia da informação, acarretando em riscos para o IPREVILLE, ou que impeçam o bom desempenho das atividades corporativas. Sempre que possível tais eventos deverão ser comunicados à Coordenadoria de TI por e-mail, contendo pelo menos, as seguintes informações:

- Detalhamento da ocorrência;
- Especificação do equipamento (PC, monitor, impressora...) ou do software (sistema operacional, suíte de aplicativos, antivírus...) conforme o caso;
- Percepção de urgência para solução da ocorrência (muito urgente, urgente, pouco urgente).

2. Classificação da Informação

Toda informação de propriedade do IPREVILLE necessita ser classificada de acordo com sua confidencialidade e relevância para o instituto, possibilitando uma classificação adequada:

a. Pública: é uma informação do IPREVILLE ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.
b. Interna: é uma informação exclusiva para processos do IPREVILLE, sem cunho público e que deve ter seu acesso, por parte de indivíduos externos ao IPREVILLE, evitado.
c. Confidencial: é uma informação crítica para os servidores do IPREVILLE ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este, composto por servidores, segurados e/ou fornecedores.
d. Informação Restrita: é toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

Todo Gerente/Coordenador deve orientar sua equipe a não circular informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

3. Declaração de comprometimento da Presidência

A Presidência do IPREVILLE declara-se comprometida em proteger o ambiente de TI do instituto, garantindo a confidencialidade, a integridade e a disponibilidade de todos os seus ativos.

4. Áreas de segurança da tecnologia da informação:

4.1 Segurança física

Conceituação – conjunto de medidas destinadas à proteção e integridade dos ativos de TI do instituto e à continuidade dos seus serviços.

Vulnerabilidades – riscos naturais (inundações, tempestades etc.), riscos acidentais (incêndios, interrupções de abastecimentos etc.), entradas não autorizadas, roubos de patrimônio, etc.

Áreas sensíveis – equipamentos, patrimônio físico, etc.

4.2 Segurança lógica

Conceituação – conjunto de medidas destinadas à proteção de recursos computacionais contra utilização indevida ou desautorizada, intencional ou não.

Vulnerabilidades – acidentes por falhas (hardware, software, aplicativos e procedimentos).

Áreas sensíveis – sistemas operacionais, sistemas gerenciadores de banco de dados, sistemas gerenciadores de rede, sistemas aplicativos e ferramentas de apoio.

4.3 Segurança das comunicações

Conceituação – conjunto de medidas destinadas à proteção das informações que trafegam por meios eletrônicos e dos recursos utilizados para esse tráfego.

Vulnerabilidades – acessos não autorizados às redes de comunicação de dados, adulteração de dados em tráfego e utilização não autorizada de informações.

Áreas sensíveis – redes de comunicação de dados, redes locais e conexões com redes externas.

4.4 Planos de continuidade

Conceituação – conjunto de planos que contemplam as atividades necessárias para a continuidade dos negócios, quando houver algum tipo de interrupção nos equipamentos críticos.

5. Diretrizes

Para o perfeito funcionamento da PSTI do IPREVILLE, as seguintes diretrizes deverão ser implementadas e seguidas:

5.1 Aspectos organizacionais e administrativos

Convém que sejam estabelecidos contratos com organizações parceiras, fornecedores de equipamentos e de infra-estrutura, fornecedores de software, fornecedores de serviços de telecomunicações, tendo como objetivo garantir ações eficazes e eficientes, quando da ocorrência de não-conformidades de segurança.

A implementação da política deve ser feita de forma gradual, em função do impacto organizacional.

É expressamente proibida a desativação ou modificação não autorizada, de forma deliberada ou não, das configurações e parâmetros dos programas utilizados na segurança do ambiente de TI do IPREVILLE, como por exemplo, antivírus e firewall.

É vedada a utilização do ambiente de TI do IPREVILLE para promoção de assédio ou para a realização de condutas de perturbação de outrem, quer seja através da linguagem utilizada, da freqüência ou tamanho de mensagens de e-mail ou através de quaisquer outras formas.

O download e instalação de quaisquer aplicativos diversos daqueles fornecidos pelo IPREVILLE, deverá ser solicitado à Coordenadoria de TI por e-mail, pela gerência, que deverá informar o nome do aplicativo, bem como, justificar sua utilização.

É vedada a utilização de aplicativos para troca e compartilhamento de arquivos, tais como uTorrent, DreaMule, BitTorrent, BitComet, Ares, e-Mule, Kazaa, Morpheus e similares.

É vedada a utilização de aplicativos para controle remoto de computadores, tais como WinVNC, UltraVNC, TeamViewer, Ammyy e similares, sem que tal utilização seja devidamente acompanhada pela Coordenadoria de TI e esteja expressamente autorizada pela gerência.

É expressamente proibida a exposição, armazenamento, distribuição, edição e manipulação de material com conteúdo pornográfico através do ambiente de TI do IPREVILLE.

5.2 Comitê de Segurança da Tecnologia da Informação (CSTI)

Deverá ser criado o CSTI – Comitê de Segurança da Tecnologia da Informação que terá a seguinte constituição: Diretor-Presidente, Gerente Administrativo, Gerente Financeiro, Gerente de Previdência, Consultor Jurídico e Coordenador de Tecnologia da Informação.

O comitê será presidido pelo Diretor-Presidente do IPREVILLE e, cada membro deverá indicar um substituto para seus impedimentos.

Principais atribuições do Comitê de Segurança da Tecnologia da Informação:

a. Analisar e decidir sobre as alterações nas regras gerais e específicas de acesso, bloqueios ou liberações para sites, downloads e tipos de arquivos externos ao IPREVILLE;
b. Analisar e decidir sobre as alterações nas regras de acesso dos usuários do domínio “ipreville.pmj” às unidades de rede do IPREVILLE;
c. Analisar e decidir sobre possíveis descumprimentos da PSTI registrados por Relatório de Descumprimento;
d. Dar suporte, perante o instituto, às iniciativas da Coordenadoria de TI.

O comitê se reunirá por convocação de seu presidente sempre que houver necessidade.

As reuniões também poderão ter como objetivo a avaliação e o aprimoramento da PSTI, a análise das ocorrências registradas através dos RD’s e as ações adotadas para sua correção e/ou sanção.

5.3 Termo de Responsabilidade e Sigilo (TRS)

O TRS – Termo de Responsabilidade e Sigilo é o documento oficial do instituto que compromete colaboradores, terceirizados e prestadores de serviço com a PSTI do IPREVILLE.

5.4 Atribuições e responsabilidades

Do ponto de vista de segurança da tecnologia da informação, são identificadas as seguintes funções genéricas, responsáveis pelo controle de acesso aos recursos de TI, com as respectivas atribuições e responsabilidades:

5.4.1 Proprietário das informações

Fica aqui definido como proprietário das informações que trafegam na rede corporativa, o Instituto de Previdência Social dos Servidores Públicos do Município de Joinville - IPREVILLE.

O IPREVILLE terá autoridade para, através do CSTI:

a. Estabelecer as regras de proteção do ambiente de TI, quanto aos bloqueios, liberações, acessos etc.;
b. Monitorar o cumprimento das regras estabelecidas.

5.4.2 Custodiante

A Coordenadoria de Tecnologia da Informação é a responsável pelo processamento, armazenamento e custódia das informações e terá a responsabilidade de:

a. Administrar os controles estabelecidos pelo proprietário da aplicação e de seus dados;
b. Administrar o acesso aos recursos dos sistemas de processamento e prover procedimentos de segurança;
c. Testar e registrar, procedimentos de HA (*High Availability*) para servidores;
d. Registrar procedimentos de *restore* de backup;
e. Controlar o acesso às informações;
f. Atender às solicitações da Presidência, Diretoria Executiva e das Gerências, quando devidamente fundamentadas;
g. Responder às não-conformidades de segurança;
h. Informar o CSTI quanto ao descumprimento da PSTI através dos RD’s.

5.4.3 Usuário da informação

É todo servidor público lotado ou comissionado no IPREVILLE, conselheiro, estagiário ou terceirizado, que tenha acesso ao ambiente de TI do IPREVILLE.

O usuário da informação terá a responsabilidade de:

a. Criar sua senha de acesso de acordo com as instruções pautadas no item 6.5.2. desta política, bem como, guardar sigilo sobre a mesma;
b. Zelar por todo acesso ao ambiente de TI executado e registrado com a sua identificação de acesso;

c. Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
d. Utilizar os recursos de TI (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;
e. Assinar o TRS - Termo de Responsabilidade e Sigilo do IPREVILLE;
f. Notificar não-conformidades de segurança.

5.4.4 Diretor Executivo e Gerente de Área

Servidor público lotado ou comissionado no IPREVILLE que ocupa cargo de direção ou gerência nas diversas áreas do instituto.

O gerente da área terá a responsabilidade de:

a. Conhecer os procedimentos de segurança em vigência;
b. Cuidar para que seus subordinados estejam informados e cientes de suas responsabilidades em relação à segurança do ambiente de TI do instituto;
c. Proceder às autorizações solicitadas desde que devidamente necessárias e fundamentadas;
d. Notificar não-conformidades de segurança.

5.5 Propriedade dos softwares aplicativos

Os sistemas aplicativos ou qualquer outro tipo de software, desenvolvidos ou adquiridos pelo IPREVILLE, são de sua exclusiva propriedade e a sua utilização se restringe a apoiar suas rotinas internas.

5.6 Utilização da Internet e do correio eletrônico (e-mail)

O acesso à Internet somente poderá ser utilizado como complemento às atividades do instituto, para enriquecimento intelectual de seus servidores ou como ferramenta para busca de informações que venham a contribuir com as atividades corporativas.

A Coordenadoria de TI poderá dispor de ferramentas para o monitoramento e gerenciamento do uso deste recurso, e poderá fazer utilização delas sempre que necessário para aplicar restrições ou bloqueios, ou para tomar quaisquer outras medidas no intuito de restabelecer a performance do ambiente de TI do instituto.

É possibilitado o uso para fins pessoais da internet como, por exemplo, para acesso a movimentação bancária, desde que fora do horário de expediente e com o consentimento da gerência.

É facultado o acesso a sites ou serviços de notícias desde que não prejudiquem o desempenho do usuário.

A utilização de programas de comunicação instantânea tais como Skype e afins, deverá ser autorizada pela gerência, por e-mail à Coordenadoria de TI, fundamentando o pedido e informando o usuário e o programa a ser liberado.

É expressamente proibido o uso de jogos on-line.

O e-mail institucional é uma ferramenta disponibilizada pelo Instituto aos seus servidores públicos, e é considerado como um ativo do Instituto, não podendo, portanto, ser utilizado para fins particulares.

É vedada a utilização do e-mail corporativo para o envio de mensagens com conteúdo ofensivo ou aquelas tipificadas como SPAM, “correntes” ou “pirâmides”. Se o destinatário das mensagens solicitar a interrupção do envio, o remetente deverá acatar tal solicitação imediatamente.

É obrigatória a utilização de assinatura no e-mail corporativo contendo, pelo menos, as seguintes informações:

a. Nome
b. Cargo
c. Telefone (Ramal)
d. Razão Social do instituto
e. Site do instituto

É obrigatória a manutenção das caixas de e-mail corporativo, evitando-se assim o acúmulo de mensagens e arquivos desnecessários. Tal manutenção poderá ocorrer através da exclusão de mensagens que não tenham cunho corporativo, que não sejam de interesse do Ipreville ou que não possuam necessidade de guarda permanente.

A utilização de programas de e-mail não corporativos tais como Gmail e Yahoo, poderá ser monitorada caso haja suspeita de conduta incompatível com o Código de Ética do Ipreville.

6. Segurança lógica

6.1 Gerenciamento de ocorrências

Quaisquer problemas que ocorram no ambiente de TI do IPREVILLE sejam eles de infra-estrutura, hardware, equipamentos de comunicação de dados, softwares e sistemas aplicativos, devem ser informados imediatamente à Coordenadoria de TI, preferencialmente por e-mail, que registrará a ocorrência com as seguintes informações básicas, através de Relatório de Atendimento: data e hora da ocorrência; usuário solicitante; descritivo da demanda; atendente; data e hora do atendimento; e, descrição da solução adotada.

6.2 Observação e planejamento dos recursos críticos

A atividade de planejamento dos recursos computacionais deve ser contínua. Devem ser observados, pelo menos a cada 15 (quinze) dias, os recursos de cada servidor ou storage considerado crítico.

6.3 Rotina de Backup

As rotinas de backup são de responsabilidade do Datacenter licitado e seguem estes critérios para todos servidores contratados:

- Modalidade incremental e a modalidade full;
- Atendem 07 (sete) dias de retenção;
- Responsabilizam-se pela administração do serviço;
- A solução atende a função de restauração “granular” de dados;
- Oferecem a restauração de até 1TB de dados em 5 minutos;
- Executam serviço de restauração (restore) com uma execução mensal sem ônus para o Ipreville.

Todos os arquivos que estão salvos na rede interna do IPREVILLE fazem parte da rotina de backup diário.

Não é realizado backup dos arquivos guardados localmente (C: da máquina), sendo o usuário orientado a salvar toda informação relevante para a operação do seu trabalho na rede do IPREVILLE.

Não é possível recuperar emails excluídos da pasta “Itens Excluídos”. É realizado backup do servidor Exchange, ou seja, em caso de necessidade é possível fazer o restore do servidor.

6.4 Controle de acesso aos recursos computacionais

6.4.1 Identificação e autenticação de usuários

a. O usuário somente terá acesso ao domínio do IPREVILLE através de uma credencial de acesso (login) e uma senha;
b. O login de acesso do usuário deve ser único;
c. A senha de acesso deve ser secreta, pessoal e intransferível, e de conhecimento exclusivo do usuário para o qual foi custodiada;
d. A senha não pode ser divulgada a terceiros, devendo-se evitar o uso de combinação simples ou óbvia na sua criação;
e. Não serão permitidas senhas para grupos de usuários;
f. Sempre que possível e necessário, os logins devem ser associados a uma determinada estação de trabalho.

6.4.2 Regras para criação de logins e senhas

a. Para serem criados logins e senhas, deve-se ter uma solicitação do setor de Folha de Pagamento, por e-mail, contendo, pelo menos, o nome do usuário, o local de trabalho, e o perfil de acesso;
b. O login criado e a primeira senha devem ser entregues para o usuário de forma sigilosa;
c. A restauração de senhas deve ser formalizada e documentada por e-mail, pelo superior imediato;
d. Não será permitida a restauração de senhas solicitadas por telefone;
e. A senha do usuário deve conter, no mínimo, oito caracteres;
f. A senha do usuário deve ser composta de números, letras e caracteres especiais (! @ # $ % *);
g. A senha do usuário deve ser substituída a cada 180 (cento e oitenta) dias;
h. A senha do usuário, quando substituída, não deverá ser similar às últimas 5 (cinco) senhas utilizadas.

6.4.3 Perfil de acesso dos usuários:

a. Cada usuário terá um perfil de acesso, indicando os arquivos, os aplicativos, as funções dos aplicativos e os dados que podem ser executados, lidos e gravados;

b. Sempre que possível, deverá ser estabelecido o mesmo perfil de acesso para um grupo de usuários comuns (mesmo setor ou função).

6.5 Trilha de auditoria

O Sistema de Gestão Previdenciária deverá manter registros, ainda que através do sistema gerenciador de banco de dados, sobre os acessos dos usuários, indicando, sempre que possível:

a. O usuário;
b. Os dados acessados;
c. Os dados alterados (informação antiga e nova);
d. A data do acesso/alteração;
e. O horário do acesso/alteração.

6.6 Trabalho remoto

Trabalhos remotos serão realizados através de VPN (*Virtual Private Network*).

Quando existir necessidade de execução de acesso remoto por qualquer servidor, deverá haver autorização prévia da gerência, por e-mail à Coordenadoria de TI, informando o nome do usuário e o período em que deverá ficar disponível tal acesso. Na ocorrência, o processo será instruído pela Coordenadoria de TI.

6.7 Acesso ao domínio corporativo

O acesso ao domínio corporativo somente será possibilitado através da utilização de login de usuário, devidamente cadastrado, mais sua senha, devidamente validada.

Os usuários somente terão acesso ao domínio nos dias úteis, das 07h00min às 18h00min.

Necessidades diversas deverão ser previamente autorizadas pela gerência responsável, bem como, comunicadas à Coordenadoria de TI através de e-mail que deverá informar o nome do usuário e o período de liberação.

6.8 High Availability para servidores

Ou Alta Disponibilidade, traduz-se como um sistema de tecnologia resistente a falhas de software, hardware e energia que tem como objetivo manter os servidores, e conseqüentemente os serviços embarcados nestes, disponíveis o máximo de tempo possível.

Esta Alta Disponibilidade é garantida através do Datacenter licitado, contendo:

- Solução de grupo motor gerador (GMG), com acionamento automático na eventualidade de interrupção no fornecimento de energia;
- Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);

- Conexões redundantes, ou seja, servidores que possuem redundância de conexões lógicas interligados por switches de rede independentes, visando reduzir número de pontos únicos de falha;
- Redundância de toda a comunicação de dados entre o Datacenter e a Internet para os diversos serviços oferecidos pelo Ipreville e consumidos pelo Instituto;
- Backbone com, no mínimo, 3 (três) saídas e rotas distintas para a internet, sendo uma delas através de PTT (Pontos de Troca de Tráfego).

7. Segurança física do ambiente de TI

7.1 Proteção dos equipamentos e da infra-estrutura

O ambiente de TI do Ipreville, no que se refere aos servidores, está hospedado em Datacenter terceirizado que responde pelas seguintes situações:

a. Deverá garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;
b. Deverá dispor de mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso da infraestrutura física do centro de serviço de hospedagem sob demanda, bem como de registros passíveis de posterior pesquisa;
c. Deverá possuir travas eletrônicas que, de acordo com a política de segurança estabelecida, separem a infraestrutura física do centro de serviço de hospedagem sob demanda em regiões diferentes e com níveis de restrição diferenciados;
d. Deverá possuir monitoramento e verificação de toda e qualquer tentativa de acesso;
e. Deverá utilizar câmeras de circuito interno de televisão, monitoradas e gerenciadas, cujas imagens possam ser posteriormente consultadas viabilizando o rastreamento de pessoas dentro do centro de serviço de hospedagem sob demanda com disponibilidade mínima de 45 dias.
f. O ambiente de TI, presente no Ipreville (ativos de rede, equipamentos e estações de trabalho, CFTV e central telefônica), deve ser segurado, pelo menos contra incêndio;
g. SLA de 24 x 7 x 365 – vinte e quatro horas por dia, sete dias por semana (incluindo feriados), trezentos e sessenta e cinco dias com início dos serviços previstos em contrato, conforme criticidade do chamado.

8. Descumprimento da P.S.T.I.

O descumprimento total ou parcial desta política será devidamente relatado ao Comitê de Segurança da Tecnologia da Informação que deverá deliberar e decidir sobre o mesmo, bem como, tomar as medidas cabíveis.

Em casos considerados como grave pelo C.S.T.I. e nos casos em que houver evidente dolo e má-fé por parte do usuário, será encaminhado para Processo Administrativo Disciplinar a fim de analisar a conduta do usuário e as penalidades decorrentes da lei.

9. Fundamentação

- Política de Segurança da Informação da PRODAM – Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo;
- Artigo “Política de Segurança da Informação: A norma ISO 17799” – CompuStream Security;
- Política de Segurança da Informação da COOABRIEL – Cooperativa Agrária dos Cafeicultores de São Gabriel, Espírito Santo;

- Decreto nº 13.362/2006 da Prefeitura Municipal de Joinville – Homologa a Política de Utilização de Internet (anexa);
- Artigo "Implementando uma Política de Segurança de TI em sua Empresa" – SCURRA Tecnologia e Inteligência;
- Política Interna de Segurança da Informação da FMTAM – Fundação de Medicina Tropical do Amazonas;
- Artigo "Segurança na Internet e Intranet" – Nuno Oliveira – EnsinoDigital.com;
- Cartilha de Segurança para Internet – Comitê Gestor da Internet no Brasil – NIC.BR;
- Política de Segurança da Informação da FIPECAFI – Fundação Instituto de Pesquisas Contábeis, Atuariais e Financeiras.

Documento assinado eletronicamente por **Guilherme Machado Casali**, **Presidente**, em 06/01/2022, às 13:15, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **0011488974** e o código CRC **6CA9FD0C**.