DECRETO N. 2.897, DE 28 DE DEZEMBRO DE 2017

Regulamenta o uso de recursos da Tecnologia da Informação disponibilizados pela Prefeitura do Município de Bertioga, e dá outras providências.

Eng.º Caio Matheus, Prefeito do Município de Bertioga, no uso das atribuições que lhe são conferidas por Lei,

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura do Município de Bertioga, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os servidores públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

CONSIDERANDO que as ações de segurança da informação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura do Município de Bertioga.

§ 1º A Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem o princípio de proteção, controle e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

§ 2º Compete à Secretaria de Administração e Finanças a coordenação das políticas de gestão da segurança da informação no Município.

Art. 2º Para efeito deste Decreto ficam estabelecidos os seguintes conceitos:

I – autenticidade: garantia que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

II – confidencialidade: garantia de que as informações sejam acessadas e reveladas somente a indivíduos, órgãos, entidades e processos devidamente autorizados;

III - dado: parte elementar da estrutura do conhecimento, computável, mas, incapaz de, por si só, gerar conclusões inteligíveis ao destinatário;

IV – disponibilidade: garantia de que as informações e os recursos de tecnologia da informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

V – gestor da informação: pessoa detentora de competência institucional para autorizar ou negar acesso à determinada informação ao usuário;

VI - incidente de segurança da informação: um evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ISO/ IEC 27001);

VII – informação: conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VIII – integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas;

IX – legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com a legislação em vigor;

X – login ou ID de usuário: identificação única do usuário, permitindo o seu acesso e controle na utilização dos recursos da tecnologia da informação;

XI - log: registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação;

XII – não repúdio: garantia de que um usuário não consiga negar uma operação ou serviço que modificou ou criou uma informação;

XIII – recursos da tecnologia da informação: recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, dentre estes podemos destacar os computadores, notebooks, tablets, pendrives, mídias, impressoras, scanners, softwares, etc;

XIV - risco: combinação de probabilidades da concretização de uma ameaça e seus potenciais impactos;

XV - segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ISO/ IEC 27001);

XVI – senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu nível de acesso aos recursos da tecnologia da informação não disponíveis ao público, de uso pessoal e intransferível;

XVII – tecnologia da informação e comunicação: solução ou conjunto de soluções sistematizadas baseadas no uso de recursos tecnológicos que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, bem como subsidiar processos que convertem dados em informação;

XVIII – usuário: funcionário, servidor, comissionado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indireta, com os órgãos e entidades da Administração Municipal;

XIX - violação: qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer das demais normas que a complemente.

Art. 3º Constituem objetivos da Política de Segurança da Informação:

I – dotar a Prefeitura do Município de Bertioga de instrumento jurídico, normativo e institucional que a capacite de forma técnica e administrativa, com o objetivo de assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sigilosas da Administração Municipal;

II – estabelecer e controlar os níveis de acesso de fornecedores externos aos sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III – assegurar a interoperabilidade entre os sistemas de segurança da informação;

IV – incorporação da cultura da segurança da informação, por todos os usuários, como um elemento essencial em seus hábitos e atitudes dentro e fora da organização.

Art. 4º A Política de Segurança da Informação instituída neste Decreto reger-se-á pelos seguintes princípios:

I – tratamento da informação como patrimônio, tendo em vista que a divulgação das informações estratégicas de qualquer natureza pertencentes à Administração deve ser protegida de forma adequada, com vistas a evitar alterações, acessos ou destruição indevidos;

II – classificação da informação, garantindo-lhe o adequado nível de proteção, considerando:

a) a avaliação da necessidade do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

b) a definição de confidencialidade da informação em consonância com as atividades desempenhadas pelo usuário, com vistas a garantir a adequada autorização de acesso pelo gestor da informação, que deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros.

III – controle de acesso às informações, tendo como orientação a classificação definida no inciso II deste artigo, respeitando a legislação vigente e considerando, ainda, que:

a) o acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades;

b) no caso de acesso a sistemas informatizados, deverão ser utilizados sistemas e tecnologias autorizadas pela Administração, por meio de usuário e senha, ambos pessoais e intransferíveis.

IV – continuidade do uso da informação, sendo necessária, para o funcionamento dos sistemas, pelo menos uma cópia de segurança atualizada e guardada em local remoto, com nível de proteção equivalente ao nível de proteção da informação original, observada as seguintes regras:

a) para a definição das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

b) os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

c) definição do nível de disponibilidade para cada serviço prestado pelos sistemas de informação, nas situações mencionadas na alínea "b" deste inciso.

V – educação em segurança da informação, devendo ser observado pelo usuário a correta utilização das informações e dos recursos computacionais disponibilizados.

Art. 5º As medidas a serem adotadas para fins de proteção da informação deverão considerar:

I – os níveis adequados de integridade, confidencialidade e disponibilidade da informação;

II – a compatibilidade entre a medida de proteção e o valor do ativo protegido;

III – o alinhamento com as diretrizes da Administração Municipal;

IV – as melhores práticas para a gestão da segurança da informação;

V – os aspectos comportamentais e tecnológicos apropriados.

Art. 6º Compete a Diretoria de Tecnologia da Informação:

I – elaborar e revisar continuamente os procedimentos e a normatização relacionada ao processo de gestão da segurança da informação;

II – avaliar propostas de modificação da Política de Segurança da Informação encaminhadas pelos demais órgãos administrativos da Administração Municipal;

III – garantir que os registros de auditoria de eventos de segurança da informação sejam produzidos e mantidos em conformidade com as normas vigentes;

IV – planejar, elaborar e propor estratégias e ações para institucionalização da política, normas e procedimentos relativos à segurança da informação;

V – avaliar a eficácia dos procedimentos relacionados à segurança da informação, propondo e implementando medidas que visem a melhoria do processo de gestão da segurança da informação no âmbito da Administração Municipal;

VI – apurar os incidentes de segurança críticos e dar o encaminhamento adequado;

VII – promover a conscientização, o treinamento e a educação em segurança da informação.

Art. 7º Compete ao gestor da informação, complementarmente às demais diretrizes estabelecidas neste Decreto:

I – subsidiar o processo de classificação da informação, de forma a viabilizar a correta definição a ela relacionada;

II – responsabilizar-se pela exatidão, integridade e atualização da informação sob sua custódia;

III – subsidiar a Diretoria de Tecnologia da Informação na compatibilização de estratégias, planos e ações desenvolvidos no âmbito da Administração Municipal relativos a segurança da informação;

IV – realizar análise de riscos em processos, em consonância com os objetivos e ações estratégicas estabelecidas pelo Poder Executivo, e atualizá-la periodicamente;

V – relatar os incidentes de segurança da informação para que sejam tomadas as devidas providências em conjunto com as áreas diretamente envolvidas.

Art. 8º O cadastro de usuário para acesso aos recursos da tecnologia da informação depende de prévio encaminhamento do formulário constante no Anexo I deste Decreto, autorizado pela chefia imediata e encaminhado para a Diretoria de Tecnologia da Informação para providências quanto ao cadastramento.

§ 1º Ao usuário será fornecido o "login ou ID do usuário", sobre o qual deverá tomar ciência e, assim, assinar o termo de responsabilidade de acesso aos recursos da tecnologia da informação, constante no Anexo II.

§ 2º Após o cadastro, o usuário deverá registrar uma senha, de uso pessoal e intransferível, que deverá ser alterada periodicamente, a qual permitirá o seu login na rede de computadores da Prefeitura e aos recursos da tecnologia da informação.

§ 3º Qualquer mudança de lotação dos usuários deverá ser comunicada imediatamente pelo setor de origem, através da chefia imediata a Diretoria de Tecnologia da Informação para que sejam realizados os ajustes necessários no seu cadastro.

§ 4º Qualquer mudança que venha a ocorrer do perfil do usuário, seja de alteração do perfil de acesso, ampliação ou exclusão de permissões deverá ser comunicado pela chefia imediata.

Art. 9º O login na rede e os demais recursos da tecnologia da informação, são de uso pessoal e intransferível, sendo que toda a e qualquer ação executada por meio de um determinado usuário, será de responsabilidade daquele a quem o login foi atribuído, cabendo-lhe, portanto, zelar pela confidencialidade de sua senha.

Art. 10. Ao perder o vínculo com a Prefeitura todos os acessos do usuário aos recursos da tecnologia da informação serão excluídos, suas contas de e-mails canceladas e seu conteúdo apagado.

Parágrafo único. Fica a Secretaria de Administração e Finanças, através da Diretoria de Recursos Humanos, responsável por repassar à Diretoria de Tecnologia da Informação, a qualquer tempo, as demissões/exonerações, do quadro de funcionários, para que as providências acima sejam tomadas.

Art. 11. É dever do usuário, em consonância com a Política de Segurança da Informação estabelecida neste Decreto:

I – zelar pelo sigilo da sua senha;

II – zelar pela segurança das informações, fechando ou bloqueando o acesso aos equipamentos de informática ou softwares quando estiver utilizando;

III – comunicar imediatamente ao seu superior hierárquico qualquer suspeita de que estejam sendo executados atos em seu nome por meio dos recursos da tecnologia da informação;

IV – zelar pela integridade física dos equipamentos de informática utilizados, evitando submetê-los a condições de riscos, mantendo-os afastados de líquidos e alimentos, não danificando as placas de patrimônio, não colando qualquer tipo de adesivo nos equipamentos ou qualquer material e/ ou utensílio que possa danificá-los, e comunicando ao órgão competente qualquer anormalidade ou defeito;

V – zelar pela segurança da informação que esteja sob sua custódia em razão de seu exercício funcional.

Art. 12. É proibido aos usuários:

I – fornecer por qualquer motivo, seu login e senha para acesso a outrem;

II – fazer uso do login e da senha de terceiro;

III – utilizar os recursos da tecnologia da informação em desacordo com os princípios éticos da Administração Pública;

IV – visualizar, acessar, expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica, racista, jogos, música, filmes e outros relacionados, por meio de uso de recursos de computadores da Prefeitura;

V – acessar sites ou serviços que representem

risco aos dados ou à estrutura de redes da Prefeitura;

VI – fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos pela Prefeitura.

Art. 13. É vedado o uso de equipamentos de informática particulares conectados à rede de informática da Prefeitura, sem a prévia autorização da Diretoria de Tecnologia da Informação.

Parágrafo único. Em todos os equipamentos utilizados na rede da Prefeitura, será instalado software de acesso remoto, sendo que a desinstalação do mesmo pelo usuário acarretará na retirada do equipamento da rede e envio de notificação ao superior hierárquico do usuário.

Art. 14. A Diretoria de Tecnologia da Informação é a única detentora e responsável pela senha de administrador dos equipamentos.

Parágrafo único. As solicitações para compartilhamento da senha de administrador dos equipamentos deverão ser encaminhadas com a devida justificativa para que seja avaliada esta necessidade em conjunto com o órgão solicitante.

Art. 15. São considerados usos inadequados dos equipamentos de informática:

I – instalar hardware em computador da Prefeitura;

II – instalar softwares de qualquer espécie em computador da Prefeitura;

III – reconfigurar a rede corporativa ou inicializa-la sem prévia autorização expressa;

IV – efetuar montagem, alteração, conserto ou manutenção em equipamentos da Prefeitura sem o conhecimento da Diretoria de Tecnologia da Informação;

V – alterar o local de instalação dos equipamentos/ hardwares de informática, sem prévia autorização;

VI – instalar dispositivo ou utilizar internet móvel, sem prévia autorização expressa;

VII – conectar equipamento particular na rede de computadores da Prefeitura, sem prévia autorização expressa;

VIII – utilizar mecanismos para burlar o usuário/ administrador, concedendo privilégios aos demais usuários;

IX – utilizar dispositivos de armazenamento externos tais como pen drive, HD externo, sem prévia autorização, mesmo com a devida autorização da Diretoria de Tecnologia da Informação, a mesma não se responsabiliza caso estes venham a queimar durante a utilização.

Art. 16. Compete exclusivamente a Diretoria de Tecnologia da Informação realizar backup diário dos dados armazenados nos servidores internos da Prefeitura.

Parágrafo único. Não compete a Diretoria de Tecnologia da Informação fazer backup diário ou periódico de informações armazenadas localmente nos computadores, porém, a mesma deverá orientar os usuários quanto as melhores práticas para realização de backups para aplicativos instalados em computadores locais e quanto a importância de salvar os arquivos mais importantes na rede da Prefeitura.

Art. 17. A Prefeitura adotará política interna de inspeção e restrição de acesso à internet, com a identificação do usuário por meio de sistema automatizado.

Art. 18. É considerado uso inadequado da internet:

I – acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente sites de conteúdo agressivo (racismo, pedofilia, nazismo, etc.), de drogas, pornografia e outros relacionados;

II – fazer download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques a programas de código malicioso em suas diferentes formas;

III – violar os sistemas de segurança da Prefeitura;

IV – tentar ou efetivamente burlar as regras definidas de acesso à internet;

V – alterar os registros de acesso à internet;

VI – realizar ataque ou invadir computadores da Prefeitura;

VII – utilizar acesso à internet provido pela Prefeitura para transferência de arquivos que não estejam relacionados às suas atividades;

VIII – divulgar informações confidenciais da Prefeitura em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas na forma da lei.

Art. 19. O chefe imediato do usuário deverá comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes da Prefeitura.

Art. 20. O usuário, a critério de seu chefe imediato e de acordo com as necessidades de serviço, poderá ter acesso a uma conta de correio eletrônico associada ao respectivo login.

§ 1° As contas oficiais de e-mail da Prefeitura devem ser utilizadas, exclusivamente, para transmitir e receber informações relacionadas às atividades administrativas.

§ 2° As contas de e-mail particulares não terão suporte da Diretoria de Tecnologia da Informação, podendo ser bloqueado o acesso sem prévio aviso.

Art. 21. As contas de e-mail terão limitado de espaço para armazenamento de mensagens, devendo o usuário efetuar a exclusão das mensagens inutilizadas, sob pena de ficar impedido automaticamente de enviar e receber novas mensagens, devendo casos excepcionais serem encaminhados à Diretoria de Tecnologia da Informação para análise e deliberação.

§ 1° As mensagens enviadas ou recebidas, incluindo seus anexos, tem limitação de tamanho, sendo automaticamente bloqueadas quando ultrapassarem esse limite.

§ 2° Os anexos às mensagens enviadas e recebidas não devem conter arquivos que não estejam relacionados às atividades administrativas ou que ponham em risco a segurança do ambiente da rede local.

§ 3° Os e-mails vão seguir o seguinte padrão:

a) pessoal: nome_registro@bertioga.sp.gov.br

b) órgão administrativo: secretaria.órgãoadmbertioga.sp.gov.br

§ 4° Com relação ao e-mail do órgão administrativo cabe salientar que o mesmo vai ter a função de "Alias", ou seja, é um e-mail que só recebe e redireciona para um e-mail pessoal, tal norma serve para identificação em caso de envio de e-mail indevido utilizando o e-mail do órgão administrativo.

Art. 22. É considerado uso inadequado ao serviço de e-mail:

I – acessar contas de e-mail de outros usuários;

II – enviar material ilegal ou não ético, comercial com mensagens do tipo corrente, spam, entretenimento e outros que não sejam de interesse da Prefeitura, bem como campanhas político-partidárias e que tenham finalidade eleitoreira;

III – enviar mensagens que possam afetar de forma negativa a Prefeitura e seus servidores públicos.

Art. 23. Não será considerado uso inadequado do e-mail a veiculação de campanhas internas de caráter social ou informativo, desde que previamente aprovado pela Diretoria de Comunicação.

Art. 24. Os usos de softwares de compartilhamento de arquivos e de troca de mensagens serão tratados em Decreto específico.

Art. 25. Todo caso de exceção às determinações da Política de Segurança da Informação deve ser analisado de forma individual, aplicável apenas

ao seu solicitante, dentro dos limites e motivos que o fundamentaram.

Art. 26. A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, indisciplina ou insubordinação, conforme o caso, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.

Art. 27. Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Bertioga, 28 de dezembro de 2017.
(PA n. 8451/17)

Eng.º Caio Matheus
Prefeito do Município