RESOLUÇÃO Nº 03/18 – CA/BERTPREV

ALEXANDRE HOPE HERRERA, Presidente do Conselho Administrativo do Instituto de Previdência Social dos Servidores Públicos do Município de Bertioga, no uso das atribuições que lhe são conferidas por Lei e

CONSIDERANDO o disposto no Decreto Municipal nº 2.897/17, publicado no BOM nº 814, de 30/12/17,

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito do BERTPREV, promovendo a proteção dos usuários, dos equipamentos, dos softwares e dos dados dos segurados.

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito do BERTPREV, 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;

CONSIDERANDO aprovação do Conselho Administrativo da Autarquia, em reunião de 21/06/2018.

RESOLVE

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito do BERTPREV.

§ 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 pelo BERTPREV.

§ 2º Compete à Coordenação Administrativo-Financeira, a coordenação das políticas de gestão da segurança da informação do BERTPREV.

Art. 2º Para efeito desta Resolução 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/ IEC27001);

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

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 edescartar 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/ IEC27001);

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 o BERTPREV;

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 o BERTPREV 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 do BERTPREV;

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 nesta Resolução, 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 ao BERTPREV 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 Coordenação Administrativa-Financeira, 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. 5° 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 do BERTPREV;

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

V – os aspectos comportamentais e tecnológicos apropriados.

Art. 6° Compete o setor 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 setores administrativos do BERTPREV;

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 à melhoria do processo de gestão da segurança da informação no âmbito do BERTPREV;

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. 7° 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 o setor de Tecnologia da Informação na compatibilização de estratégias, planos e ações desenvolvidos no âmbito do BERTPREV, relativos à 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. 8° O cadastro de usuário para acesso aos recursos da tecnologia da informação depende de prévio encaminhamento do formulário constante no Anexo I desta Resolução, autorizado pela chefia imediata e encaminhado para o setor de Tecnologia da Informação para providências quanto ao cadastramento.

§ 1° 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.

§ 2° 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 do BERTPREV e aos recursos da tecnologia da informação.

§ 3° Qualquer mudança de lotação dos usuários deverá ser comunicada imediatamente pelo setor de origem, através da Coordenação, ao setor de Tecnologia da Informação para que sejam realizados os ajustes necessários no seu cadastro.

§ 4° 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. 9° O login na rede e os demais recursos da tecnologia da informação, são de uso pessoal e intransferível, sendo que 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 o BERTPREV, 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 o setor de Recursos Humanos do BERTPREV, responsável por repassar ao setor 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 nesta Resolução:

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 não 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 ou prestação de serviço.

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 deterceiro;

III – utilizar os recursos da tecnologia da informação em desacordo com os princípios éticos do BERTPREV;

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 do BERTPREV;

V – acessar sites ou serviços que representem risco aos dados ou à estrutura de redes do BERTPREV;

VI – fazer cópias não autorizadas dos softwares desenvolvidos, locados ou adquiridos pelo BERTPREV.

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

Parágrafo único. Em todos os equipamentos utilizados na rede do BERTPREV, 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. O setor de Tecnologia da Informação é o único detentor 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 do BERTPREV;

II- instalar softwares de qualquer espécie em computador do BERTPREV;

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

IV – efetuar montagem, alteração, conserto ou manutenção em equipamentos do BERTPREV sem o conhecimento do setor 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 do BERTPREV, 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 e mesmo com a devida autorização do setor de Tecnologia da Informação, a mesma não se responsabiliza caso estes venham a queimar durante a utilização.

Art. 16. Compete exclusivamente ao setor de Tecnologia da Informação realizar backup diário dos dados armazenados nos servidores internos do BERTPREV.

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

Art. 17. O BERTPREV 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 com softwares maliciosos em suas diferentes formas;

III – violar os sistemas de segurança do BERTPREV;

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 do BERTPREV;

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

VIII – divulgar informações confidenciais do BERTPREV 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 dalei.

Art. 19. A chefia imediata do usuário deverá comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes do BERTPREV.

Art. 20. O usuário, a critério de sua Coordenação 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 do BERTPREV devem ser utilizadas, exclusivamente, para transmitir e receber informações relacionadas às atividades administrativas.

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

Art. 21. As contas de e-mail terão limite 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 ao setor 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@bertprev.sp.gov.br

b) setorial:setor@bertprev.sp.gov.br

§ 4° O e-mail do órgão administrativo terá a função de "Alias", isto é, um e-mail que só recebe e redireciona para um e-mail pessoal, para identificação em caso de envio de mensagem indevida, utilizando-se do 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 do BERTPREV, bem como campanhas político-partidárias e que tenham finalidade eleitoreira;

III – enviar mensagens que possam afetar de forma negativa o BERTPREV 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 Coordenação Administrativo-Financeira.

Art. 24. Os usos de softwares de compartilhamento de arquivos e de troca de mensagens serão tratados em Resolução específica.

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. As empresas prestadoras de serviço, que tenham acesso às informações do BERTPREV, deverão por meio do sócio responsável, assinar o termo de responsabilidade, anexo III

Art. 27. 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.

Bertioga, 21 de junho de 2018.

Alexandre Hope Herrera
Presidente

ANEXO I
FICHA DE SOLICITAÇÃO DE INCLUSÃO/ EXCLUSÃO DE ACESSOS A SERVIÇOS DE TI

1 – INFORMAÇÕES GERAIS			
SETOR SOLICITANTE		DATA	
NOME COMPLETO DO USUÁRIO			
USUÁRIO DA REDE		Obs.: Caso seja o 1º cadastro do funcionário, não preencher este campo. O nome do usuário da rede será informado após o cadastro.	
SOLICITAÇÃO DE:	( ) INCLUSÃO/ ALTERAÇÃO ( ) DESBLOQUEIO* EXCLUSÃO* DE USUÁRIO POR MOTIVO DE: ( ) DESLIGAMENTO ( )OUTRO:_____ BLOQUEIO* POR MOTIVO DE: ( ) FÉRIAS ( ) MAUUSO ( )OUTRO:_____		

* Para esta opção, não é necessário preencher o item 2.

2 – SERVIÇOS DISPONÍVEIS (Preencher somente para solicitações de inclusão ou modificação de acessos. Este campo deverá ser preenchido pelo chefe imediato, o qual definirá quais serviços o usuário terá direito de acesso).		
CONTA PARA ACESSO AOS COMPUTADORES DA REDE	( ) PERMITIDO	( ) NÃO PERMITIDO
PERMISSÃO DE ACESSO A INTERNET	( ) PERMITIDO	( ) NÃO PERMITIDO
CORREIO ELETRÔNICO (E-MAIL)	( ) PERMITIDO	( ) NÃO PERMITIDO
SISTEMAS DE INFORMAÇÃO:	( ) PERMITIDO	( ) NÃO PERMITIDO

3 - AUTORIZAÇÃO	
ASSINATURA DO USUÁRIO Assinando o presente, o usuário aceita todas as normas estabelecidas pelo BERTPREV.	
ASSINATURA DO COORDENADOR	

4 – CAMPOS A SEREM PREENCHIDOS PELA TI			
DATA RECEBIMENTO		DATA ATENDIMENTO	
ASSINATURA DO RESPONSÁVEL			

ANEXO
II
TERMO DE RESPONSABILIDADE
ACESSO AOS RECURSOS TECNOLOGIA DA INFORMAÇÃO

Eu,_____, declaro haver solicitado acesso aos Recursos da Tecnologia da Informação e comprometo-mea:

Acessar a internet/intranet somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege o acesso à internet/intranet e utilização de*e-mails*;

1. Utilizar a caixa postal (e-mail) colocada a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, às normas e às disposições contidas na instrução normativa que rege o acesso à internet/intranet e utilização de e-mails;

2. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

3. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

4. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bem como encerrar a seção do cliente de correio, garantindo, assim, a impossibilidade de acesso indevido por terceiros;

5. Não revelar minha senha de acesso à internet/intranet e de minha caixa postal (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

6. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenhaacesso.

Declaro, ainda, estar plenamente esclarecido e consciente das cláusulas que regem a Resolução nº
_____, enfatizando, entre outras,que:

1. Não é permitida a navegação em *sites* pornográficos, defensores do uso de drogas, de pedofilia ou *sites* de cunho racista esimilares;

2. É de minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações contidas em minha caixa postal (*e-mail*), devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas no sistema de correio, sendo proibida a exploração de falhas ou vulnerabilidades porventuraexistentes;

3. O acesso à informação de minha caixa postal (*e-mail*) não me garante direito sobre ela, uma vez que faço uso para melhor desempenhar minhas atividades administrativas, nemme confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes ao BERTPREV;

4. Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos por meio do uso de minha caixa postal (*e-mail*), a qual tenho acesso, para outros servidores não envolvidos nos trabalhosexecutados;

5. Devo alterar minha senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmentedescobertas;

6. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados;

7. Cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação, de suas diretrizes, bem como deste Termo deResponsabilidade.

Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional a revelação de segredo do qual me apropriei em razão do cargo, sendo crime contra a Administração Pública a divulgação a quem não seja de direito, das informações a(s) qual(is) tenho acesso, estando sujeito às penalidades previstas em lei;

Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda quehabilitado;

Constitui infração funcional e penal enviar ou facilitar o envio por terceiros de *e-mails* falsos, ficando o infrator sujeito à punição com a demissão, conforme responsabilização por crime contra a Administração Pública, tipificado nos artigos 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei nº 2.848, de1940).

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos anteriormente descritos,
comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

Local _____ data __/__/____

_____
Assinatura

ANEXO
III
TERMO DE RESPONSABILIDADE
ACESSO AOS RECURSOS TECNOLOGIA DA INFORMAÇÃO

Eu,_____, responsável pela empresa _____, declaro estar plenamente esclarecido e consciente das cláusulas que regem a Política de Segurança da Informação do BERTPREV, e comprometo-me a garantir que os sócios ou colaboradores da empresa cumpram o que segue:

7. Não fornecer ou facilitar o acesso, às informações ou banco de dados do Instituto, pois ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração penal a revelação de segredo do qual me apropriei em razão de prestação de serviço, sendo crime contra a Administração Pública a divulgação a quem não seja de direito, das informações a(s) qual(is) a empresa tenha acesso, estando sujeito às penalidades previstas em lei;

8. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento, salvo em decorrência de decisão competente na esfera legal ou judicial;

9. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas nãoautorizadas;

10. Não revelar ou facilitar o acesso à qualquer senha do Instituto;

11. Responder, em todas as instâncias, pelas consequências das ações ou omissões por parte da empresa que sou responsável, que possam pôr em risco ou comprometer a exclusividade de conhecimento das informações que a empresa tenha acesso.

12. Cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos anteriormente descritos,
comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

Local _____ data __/__/____

_____
Assinatura