RESOLUÇÃO Nº 03, DE 19 DE DEZEMBRO DE 2019.

Dispõe sobre a Política da Segurança da Informação no âmbito do Instituto de Previdência do Estado do Rio Grande do Sul – IPE Prev.

O **DIRETOR PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DO ESTADO DO RIO GRANDE DO SUL – IPE Prev**, no uso das atribuições conferidas pelo art.14, inciso VII, da Lei Complementar nº 15.143, de 5 de abril de 2018,

considerando o disposto no Decreto nº 52.616, de 19 de outubro de 2015, que institui a Política de Tecnologia da Informação e Comunicação – TIC-RS, e no Decreto n° 54.581, de 25 de abril de 2019, que dispõe sobre a Política de Governança e Gestão da Administração Pública Estadual;

considerando que os sistemas de informação são mecanismos de gestão, baseados em Tecnologia da Informação e Comunicação - TIC e visam conduzir, facilitar, agilizar e aperfeiçoar a tomada de decisão nas organizações; e

considerando as normas de segurança da informação ABNT NBR ISO/IEC 27002:2013 e NBR ISO/IEC 27001:2013;

RESOLVE:

Art. 1º O uso dos recursos de Tecnologia da Informação e Comunicação – TIC, no âmbito do Edifício-sede do Instituto de Previdência do Estado do Rio Grande do Sul - IPE Prev, será realizado na forma desta Resolução, com a finalidade de estabelecer condições para o aprimoramento da gestão de TIC, assim como comunicar boas práticas no uso dos seus recursos, pressupondo a garantia da confidencialidade, da integridade, da autenticidade, da irretratabilidade e da disponibilidade dos ativos de informação.

Art. 2º Para os efeitos desta Resolução, considera-se:

I - acesso imotivado: aquele realizado para fins estranhos às tarefas funcionais do usuário;

II - acesso lógico: operação de consulta e/ou atualização de dados e informações em um sistema;

III - confidencialidade: princípio de segurança que estabelece restrições ao acesso e à utilização da informação;

IV - conta de usuário: conjunto de direitos e propriedades de um usuário que lhe provê acesso a recursos de um sistema;

V - direito de acesso: conjunto de permissões dado a um usuário para realizar tarefas em um sistema informatizado;

VI - gestor do sistema: responsável pela definição, pela manutenção e pelo acesso do respectivo Sistema;

VII - incidente de segurança: não atendimento de uma norma e/ou procedimento de segurança;

VII - integridade: princípio de segurança que trata da confiabilidade da informação;

IX - "spam": envio de mensagem não solicitada;

X - rede do IPE Prev: conjunto de programas, de estações de trabalho, de equipamento servidores, de equipamentos de comunicação, de infraestrutura e afins, colocado à disposição de seus servidores para o exercício de suas funções;

XI - sítio: página da "internet" possível de ser acessada via navegador padrão ou outro programa utilizando-se da suíte de protocolos TCP/IP; e

XII - usuário: pessoa física cadastrada em sistemas que estejam sendo executados na rede de computadores, e habilitada para o acesso a informações.

DA ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 3º O Grupo Governança de Tecnologia da Informação e Comunicação - GGTIC/IPE Prev é responsável pela administração dos recursos de Tecnologia da Informação e Comunicação no âmbito de todo o IPE Prev.

§ 1º Poderão ser delegados pelo GGTIC/IPE Prev, com chancela do Diretor-Presidente do IPE Prev, a terceiros, serviços e funções que não impliquem no comprometimento da segurança dos dados existentes.

§ 2º Os terceiros contratados estarão obrigados ao cumprimento de todas as normas desta Resolução.

DA UTILIZAÇÃO DA REDE DE COMPUTADORES, DE EQUIPAMENTOS E DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO

Art. 4º A utilização da rede de computadores do IPE Prev deverá ser feita por usuários devidamente cadastrados e identificados.

§ 1º Nas redes, assim como nos computadores, serão utilizados apenas programas e aplicativos homologados, sendo vedada a instalação de sistemas sem a prévia autorização do Serviço de Suporte de Informática.

Art. 5º Todos os servidores deverão estar informados sobre as Políticas de Segurança da Informação – PSI, sendo obrigatória a assinatura do Termo Individual de Responsabilidade, conforme anexo único, cuja assinatura é condição para acesso aos sistemas.

Art. 6º O acesso aos sistemas e às informações estará disponível apenas às pessoas autorizadas.

§ 1º A autorização de acesso deverá ser requerida pela chefia imediata do usuário, por meio eletrônico, e não confere o direito imotivado aos sistemas e informações.

§ 2º As credenciais de acesso aos sistemas somente serão fornecidas mediante formalização do pedido de acesso.

§ 3º A Gerência de Recursos Humanos deverá informar ao Serviço de Suporte de Informática qualquer mudança no exercício ou na lotação do usuário, para que seja providenciada a alteração ou a desativação da conta, quando for o caso, bem como alterações que venham a afetar o seu cadastro, tais como unidade de exercício, cargo ou função, etc.

Art. 7º Os usuários dos sistemas de informação deverão:

I - verificar os procedimentos de segurança previstos nesta Resolução, ficando diretamente responsáveis pelas consequências decorrentes de práticas que danifiquem ou que coloquem em risco os sistemas de informação e os arquivos de dados; e

II - comunicar imediatamente ao Serviço de Suporte de Informática os procedimentos, os equipamentos, os arquivos ou as mensagens de comportamento anômalo ou inadequado.

Art. 8º Os acessos aos sistemas de informática que não estejam relacionados com as atividades funcionais do usuário serão considerados inadequados e são vedados**,** quando:

I – implicarem comprometimento da segurança da rede;

II – caracterizarem-se como atividades comerciais com fins particulares, incluindo oferta ou pedido de serviços ou de mercadorias de vendedores “on-line”; e

III – praticadas condutas contrárias à ética, à moral e ao decoro, inclusive em redes sociais e plataformas eletrônicas.

Art. 9º A utilização indevida da rede de computadores, de equipamentos e de sistemas de tecnologia da informação identificada por qualquer usuário, deverá ser comunicada expressamente ao GGTIC/IPE Prev, por meio eletrônico, para a análise e a avaliação das medidas cabíveis.

Art. 10. Fica vedado aos servidores do IPE Prev o uso de equipamentos móveis particulares, como telefones celulares, “notebook”, “tablets” e similares, utilizando a rede e os sistemas do IPE Prev, para fins particulares.

Parágrafo único. A utilização indevida dos equipamentos, “software” e acessos deverá ser comunicada ao GGTIC/IPE Prev.

DAS CONTAS DE USUÁRIOS E DAS SENHAS DE ACESSO

Art. 11. As credenciais de acesso, compostas por conta de usuário e senha, serão fornecidas pelos gestores dos sistemas mediante a solicitação formal da chefia imediata, por meio eletrônico, com os seguintes regramentos:

I – as contas de usuários e senhas seguirão o padrão adotado pelo Serviço de Suporte de Informática;

II - o prazo para a criação das contas de usuário e de senhas é de até 48 horas, após o início do exercício;

III - as credenciais de acesso a sistemas e as senhas são pessoais e intransferíveis;

IV – é proibida a utilização de contas alheias para realizar acessos;

V - os sistemas poderão ser programados para expirar a senha dos usuários com periodicidade determinada pelos gestores dos sistemas;

VI - ao expirar a senha, o próprio usuário deverá escolher uma nova senha de acesso;

VII - o usuário poderá, a qualquer momento, trocar a sua senha, provocando o reinício de contagem do prazo de expiração;

VIII - os gestores dos sistemas definirão a reutilização da(s) última(s) senha(s) do usuário quando da troca de senha;

IX - é proibida a criação e/ou utilização de programas que tenham o objetivo de obter senhas de outros usuários;

X – o desbloqueio ou reinicialização das senhas de acesso deverá ser solicitado pelo usuário ou por sua chefia imediata, por meio eletrônico; e

XI – nenhum administrador terá acesso à senha de qualquer usuário.

§ 1º As credenciais de usuário serão desativadas sempre que cessar a necessidade de serviço que deu origem a sua criação, devendo a chefia imediata do usuário informar ao Serviço de Suporte de Informática no prazo máximo de 48 horas, o qual terá o prazo de 24 horas para efetuar o cancelamento.

§ 2º É responsabilidade do usuário a guarda e a confidencialidade de sua senha, bem como qualquer operação realizada com as suas credenciais.

Art. 12. O controle de acesso lógico deverá:

I - proteger as informações dos sistemas informatizados contra o uso não autorizado;

II - auxiliar na detecção de violação de segurança;

III – assegurar a recuperação nas situações de falha;

IV - permitir contabilização das informações definidas pelos gestores dos sistemas; e

V - preservar os dados relativos às transações realizadas nos sistemas, com a identificação do usuário, do local, da data e do horário de acesso.

Art. 13. Os gestores dos sistemas, relativamente ao controle de acesso lógico, possuem as seguintes atribuições:

I - definir e classificar os perfis de usuários;

II - manter atualizada a relação dos perfis, com seus respectivos usuários e ações;

III - definir, quando necessário para a atribuição de direitos de acesso, as unidades administrativas nas quais os usuários poderão trabalhar;

IV - definir as informações de acesso e de operações realizadas no sistema que devam ser armazenadas, bem como o prazo de retenção das mesmas para o acesso “on-line” e “batch”; e

V - manter as contas de usuários do sistema.

Art. 14. O usuário perderá o direito de acesso à rede a contar da comunicação:

I – do desligamento de suas atividades no órgão;

II – da licença para tratar de interesses particulares; e

III - da aposentadoria, da exoneração, da demissão ou do falecimento.

Parágrafo único. É responsabilidade da Gerência de Recursos Humanos comunicar imediatamente as hipóteses acima descritas ao Serviço de Suporte de Informática, o qual deverá atender a solicitação em até 48 horas.

DO CONTROLE DE ACESSO FÍSICO AOS SERVIDORES

Art. 15. Equipamentos servidores, equipamentos ativos de rede, mídias de instalação de programa e mídias de “backup”, considerados Ativos de Informação com maior criticidade, serão mantidos em locais com acesso controlado.

§ 1º O controle e inventários destes ativos serão de responsabilidade do Serviço de Suporte de Informática.

§ 2º A consolidação do inventário dos equipamentos de Tecnologia da Informação será realizada pelo sistema APE - Administração do Patrimônio do Estado.

Art. 16. O acesso físico a sala de controle dos servidores, "switches", "nobreaks" e equipamentos ativos de rede será feito somente com acompanhamento de pessoal autorizado e devidamente identificado no Serviço de Suporte de Informática.

Art. 17. A configuração, as condições físicas e qualquer alteração da rede elétrica ou lógica, bem como a segurança dos equipamentos servidores, serão definidas previamente pelo Serviço de Suporte de Informática.

Art. 18. Deverão ser solicitadas ao Serviço de Suporte de Informática, as mudanças de "layout", a instalação ou a reinstalação dos equipamentos envolvidos, que deverão ser realizadas somente por pessoal autorizado.

DO CORREIO ELETRÔNICO

Art. 19. Será disponibilizado aos usuários o serviço de correio eletrônico, exclusivamente com finalidades de serviço.

Parágrafo Único. É obrigação de todo usuário acessar sua caixa de correio eletrônico nos dias de exercício ordinário de suas atividades.

Art. 20. O Serviço de Suporte de Informática definirá os limites de armazenagem de cada usuário para o serviço de correio eletrônico, utilizando como parâmetros as limitações de recursos financeiros, infraestrutura e "hardware".

§ 1º É responsabilidade do usuário efetuar a manutenção de sua caixa de correio de eletrônico, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

Art. 21. O GGTIC/IPE Prev e o Serviço de Suporte de Informática poderão fazer análise do uso do correio eletrônico, e se necessário for, adotar medidas para corrigir e adequar o uso dos limites.

Art. 22. É considerado uso indevido do correio eletrônico:

I - tentativa de acesso não-autorizado ao correio eletrônico de terceiros;

II - envio de informações, inclusive senhas, para as pessoas ou organizações não-autorizadas;

III - envio de material obsceno, ilegal ou não-ético, de propaganda comercial, de propaganda política, de correntes, de jogos de computador, de “spam” e de “hoax”;

IV - vídeos que não sejam objeto de serviço;

V - envio proposital de mensagens contendo vírus ou qualquer forma de rotinas de programação prejudiciais ou danosas às estações de trabalho, aos equipamentos servidores e/ou ao sistema de correio; e

VI - outras ações que possam afetar de forma negativa a rede, os servidores, os fornecedores e os parceiros.

Art. 23. O agendamento de compromissos entre funcionários do IPE Prev será feito preferencialmente por meio de serviço disponibilizado dentro do correio eletrônico corporativo.

Art. 24. As comunicações em objeto de serviço serão, preferencialmente, realizadas via correio eletrônico pelos servidores do IPE Prev e deverão ser efetuadas na respectiva caixa funcional do usuário, vedada a utilização de correio eletrônico pessoal para finalidades laborativas.

Parágrafo Único. Não configura motivo suficiente para o não atendimento de cumprimento ou dever funcional a ausência de leitura de comunicação realizada pelo correio eletrônico.

Art. 25. As caixas de correio eletrônico serão bloqueadas para acesso pelo Serviço de Suporte de Informática em até 48 horas nas hipóteses do art. 14.

§ 1º O acesso às caixas bloqueadas somente será autorizado mediante solicitação fundamentada, dirigida ao Diretor-Presidente do IPE Prev, que decidirá à luz de análise de parecer emitido pelo GGTIC/IPE Prev.

§ 2º Após três meses do bloqueio será excluída definitivamente a caixa de correio eletrônico que estiver bloqueada pelo Serviço de Suporte de Informática, exceto se decidir, em contrário, qualquer um dos Diretores do IPE Prev, justificadamente e com a anuência do Diretor-Presidente e do GGTIC/IPE Prev.

DA POLÍTICA ANTIVÍRUS

Art. 26. A aplicação da política antivírus é executada pelo Serviço de Suporte de Informática em observância com as políticas de TIC do Estado e engloba:

I – a escolha das ferramentas antivírus, por meio de comparativos de segurança e serviços associados;

II – a homologação e a configuração das ferramentas de antivírus;

III – a atualização automática do antivírus nos equipamentos da rede do IPE Prev;

IV - o acompanhamento do correto funcionamento das ferramentas escolhidas e de sua atualização automática nos equipamentos; e

V - a adoção de medidas e de configurações que preservem a integridade dos dados e a disponibilidade dos serviços na rede.

Art. 27. Os equipamentos do IPE Prev deverão possuir permanentemente antivírus instalado em sua totalidade, cuja atualização será realizada automaticamente, via rede.

§ 1º É vedado ao usuário desabilitar o antivírus de seu equipamento.

§ 2º Caso o usuário perceba que seu computador estiver sem antivírus ou o agente de monitoramento se encontrar desativado, deverá abrir, imediatamente, um chamado técnico.

DO ARMAZENAMENTO DE DADOS E BACKUP

Art. 28. Será disponibilizada para cada setor uma pasta de armazenamento de arquivos de uso comum em equipamento servidor, cuja denominação é "Unidade X:\".

§ 1º O Serviço de Suporte de Informática configurará o acesso a "Unidade X:\", em função da lotação ou do exercício do usuário.

§ 2º Todos os arquivos serão alcançados pela política de cópia de segurança e pela política de antivírus adotada, dentro da disponibilidade de recursos de armazenamentos.

§ 3º O Serviço de Suporte de Informática definirá os limites de armazenagem, usando como parâmetros as limitações de infraestrutura, de “hardware” e de recursos financeiros.

Art. 29. É vedado aos usuários o armazenamento de documentos, de fotos, de vídeos e de materiais que não tenham correlação com as atividades funcionais pertinentes.

§ 1º O usuário que não atender o disposto no “caput” deste artigo será notificado e o Serviço de Suporte de Informática poderá excluir compulsoriamente os arquivos.

§ 2º O Serviço de Suporte de Informática não se responsabilizará por arquivos de trabalho ou pessoais gravados localmente nos equipamentos.

Art. 30. O "backup" dos arquivos, dos sistemas e dos dados do IPE Prev será efetuado em servidores dedicados a esta função na Companhia de Processamento de Dados do Estado do Rio Grande do Sul - PROCERGS.

§ 1º Se houver perda de um arquivo, o Serviço de Suporte de Informática fará a verificação da cópia de segurança dos dados juntamente à PROCERGS e solicitará restauração das informações, se necessário, por chamado técnico.

§ 2º O "backup" mantido em servidores na PROCERGS segue política de segurança e será efetuado diariamente.

DAS RESPONSABILIDADES INSTITUCIONAIS E FUNCIONAIS

Art. 31. É responsabilidade de todo usuário zelar pela integridade, pela confidencialidade e pela disponibilidade dos dados, das informações e dos sistemas, devendo comunicar qualquer anormalidade ao Serviço de Suporte de Informática.

§ 1° O Serviço de Suporte de Informática elaborará um relatório e informará ao GGTIC/IPE Prev quaisquer irregularidades, desvios ou falhas identificadas.

§ 2º É vedada a exploração de falhas ou de vulnerabilidades porventura existentes nos sistemas.

§ 3º O acesso à informação não garante direito sobre a mesma, não confere autoridade para liberar acesso a outras pessoas nem supõe autorização para divulgá-la.

§ 4º É responsabilidade da chefia imediata do usuário iniciar ação corretiva apropriada para corrigir desvios com relação às normas desta Resolução.

Art. 32 O descumprimento das disposições desta Resolução deverá ser administrativamente apurado, sem prejuízo das responsabilidades penal e civil, especialmente:

I - acesso imotivado;

II - divulgação indevida de dados;

III – repasse de informações estratégicas das quais possui conhecimento em razão do cargo;

IV - divulgação de informações protegidas pelo sigilo; e

V - falta de cuidado na guarda e na utilização da senha ou empréstimo a outro usuário, ainda que habilitado.

Parágrafo único. Constatada a ocorrência de alguma das hipóteses dos incisos do caput, poderá haver a suspensão cautelar do acesso do usuário à rede, mediante justificativa pelo GGTIC/IPE Prev.

DA UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

Art. 33. As estações de trabalho da rede serão disponibilizadas aos usuários para a realização de suas atividades funcionais.

§ 1º É dever do usuário zelar pela conservação e pela correta utilização dos equipamentos da rede.

§ 2º - É recomendado aos usuários das estações de trabalho:

I - evitar realizar transferências de arquivos muito grandes;

II - evitar acesso a sítios de "internet" com conteúdo duvidoso, não confiável ou falso;

III - evitar desconectar cabos ou periféricos, a não ser sob orientação do Serviço de Suporte de Informática; e

IV - manter bebidas e alimentos distantes dos equipamentos da rede.

Art. 34 - É vedado aos usuários das estações de trabalho:

I - acessar diretórios ou pastas de outros usuários sem autorização, ainda que estejam liberados para a leitura;

II - instalar ou desinstalar quaisquer programas nos computadores, sem prévia autorização expressa;

III - desenvolver e/ou disseminar vírus de computador nos equipamentos da rede;

IV - utilizar os equipamentos da rede em ações incompatíveis com as atividades funcionais;

V - utilizar jogos nos equipamentos da rede;

VI – permitir o acesso aos equipamentos da rede por pessoas não autorizadas;

VII - a abertura ou o acesso ao interior de qualquer equipamento da rede, sob qualquer pretexto, inclusive o de dar manutenção no equipamento;

VIII - o armazenamento de arquivos que não tenham relação com atividades funcionais; e

IX - a utilização de equipamentos particulares, em objeto de serviço, conectado a rede interna do IPE Prev.

DO MONITORAMENTO E DA AUDITORIA

Art. 35. Será permitido aos gestores dos sistemas monitorar e controlar as atividades do usuário, quando houver indícios de uso indevido dos sistemas de informação.

Parágrafo único. Havendo indícios de incidente de segurança, poderá haver averiguação inicial.

Art. 36 - Os gestores dos sistemas realizarão auditoria quando formalizado requerimento pela chefia imediata, pelo Serviço de Suporte de Informática ou pelo GGTIC/IPE Prev.

Parágrafo único. Os gestores dos sistemas, sob pena de responsabilidade funcional, ao realizar a auditoria, deverão registrar:

I - o usuário;

II - o motivo;

III - a data e a hora de início;

IV - a data e a hora do final; e

V - o resultado da inspeção.

CONSCIENTIZAÇÃO DE USUÁRIOS

Art. 37. A Política de Segurança da Informação será disponibilizada na página do IPE Prev na “internet” e “intranet” para acesso e conhecimento de seu inteiro teor aos usuários.

§ 1º Cartilhas de segurança, separadas por assuntos, serão disponibilizadas na “intranet”, a fim de conscientizar os usuários de seus direitos e responsabilidades.

§ 2º Serão desenvolvidos treinamentos, os quais ficarão disponíveis aos usuários na “intranet”, para o desenvolvimento de uma cultura de valorização da segurança da informação no IPE Prev.

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 38. Os contratos de prestação de serviços relacionados aos sistemas informatizados devem conter cláusulas que viabilizem a adoção e a manutenção das normas de segurança instituídas por esta Resolução.

Art. 39. O GGTIC/IPE Prev poderá sugerir à Diretoria Executiva a adoção de procedimentos e recomendações de uso, bem como os aspectos de segurança específicos de cada sistema.

Art. 40. As regras de uso de correio eletrônico e redes sociais serão definidas em instrumento próprio.

Art. 41. O uso dos recursos de Tecnologia da Informação e Comunicação – TIC, em agências e escritórios no interior do Estado será regulamentado oportunamente.

Art. 42. Esta Resolução entra em vigor na data de sua publicação no site do IPE Prev.

JOSÉ GUILHERME KLIEMANN,
Presidente do IPE Prev.