Diário Oficial do Estado de Rondônia nº 65
Disponibilização: 07/04/2022
Publicação: 07/04/2022

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdencia dos Servidores Publicos - IPERON

RESOLUÇÃO N. 29/2022/IPERON-GAB

Porto Velho, 05 de abril de 2022.

Atualiza a Política Corporativa de Segurança da Informação (PCSI/IPERON) no âmbito do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon, e REVOGA A RESOLUÇÃO NORMATIVA Nº. 001/GAB/IPERON, DE 30 DE ABRIL DE 2015 (DOE Nº. 2700).

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA no uso de suas atribuições que lhe confere o Decreto de 18 de janeiro de 2022, publicado no DOE n. 16 de 26 de janeiro de 2022, encaminha para publicação a Resolução da Política de Segurança da Informação (PCSI/IPERON) no âmbito do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon;

CONSIDERANDO as atribuições definidas no Decreto nº 13.627, de 21/05/2008, especificamente o Artigo 8º, inciso XIX;

CONSIDERANDO que o IPERON gera, adquire ou absorve informações no exercício de suas competências Constitucionais, legais e regulamentares, e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO que as informações no IPERON são armazenadas em diferentes suportes, veiculadas por diferentes formas, tais como meio impresso, eletrônico e microforma, e, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO que a adequada gestão da informação precisa nortear todos os processos de trabalho e unidades do IPERON e deve ser impulsionada pela Política Corporativa de Segurança da Informação;

CONSIDERANDO que a NBR ISO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

CONSIDERANDO que o manual do PRÓ-GESTÃO descreve a necessidade de Manter Comitê de Segurança da Informação, no âmbito do ente federativo ou do RPPS, como grupo multidisciplinar com o intuito de definir e apoiar estratégias necessárias à implantação, manutenção e aprimoramento da Política de Segurança da Informação, que deverá ser revista periodicamente, no mínimo a cada 2 (dois) anos, conforme prescrição em normativo interno.

RESOLVE:

Art. 1°. Atualizar a Política Corporativa de Segurança da Informação do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia (PCSI/IPERON) que observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º. A PCSI/IPERON alinha-se às estratégias do Instituto e tem por objetivo garantir a autenticidade, a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pelo IPERON.

Parágrafo único. O propósito da PCSI é estabelecer diretrizes para as normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações.

CAPÍTULO II

DOS CONCEITOS

Art. 3º. Para os efeitos desta Resolução, considera-se:

I - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

II - Segurança da informação: proteção da informação contra ameaças para garantir sua continuidade, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

III - Gestor da informação: unidade ou projeto do IPERON que, no exercício de suas competências, produz ou obtém, de fonte externa ao Instituto, informações de propriedade de pessoa física ou jurídica;

IV – Custo diante: pessoa física, unidade ou projeto do IPERON que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Instituto;

V - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações ou ameaçar a segurança da informação.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º. A segurança da informação no IPERON abrange aspectos físicos, tecnológicos humanos da organização e orienta-se pelos seguintes princípios:

I - Confidencialidade: Garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para tal;

II – Disponibilidade: Garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

III - Integridade: Garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.

IV - Respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

V - Fortalecimento da cultura de segurança da informação na sociedade;

CAPÍTULO IV
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Seção I
Dos critérios para uma política de segurança eficiente

Art. 5º. A PCSI/IPERON orientar-se-á pelo seguinte:

I – O IPERON, por meio de suas diretrizes, será instruído mediante todas as ações de segurança, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos tecnológicos do IPERON.

II - Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao IPERON;

III - Todos os recursos de informação do IPERON devem ser projetados para que seu uso seja consciente e responsável;

IV - Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos;

V - Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários.

VI - Todo o acesso a redes e sistemas do Instituto deverá ser feito por meio de login de acesso único, pessoal e intransferível;

VII - O IPERON pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pelo Instituto;

VIII - Cada usuário é responsável pela segurança das informações dentro do IPERON, principalmente daquelas que estão sob sua responsabilidade;

IX - Esta Política Corporativa de Segurança da Informação será implementada no IPERON por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

§1º. Em casos excepcionais, não sendo possível possuir as informações previstas no inciso I, deverá ser explícita e formalizada justificativa entre as partes;

§2º. A operação constante do inciso IV só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade;

Seção II
Dos objetivos

Art. 6º. Para os efeitos desta Resolução, os Objetivos da PCSI/IPERON, além de buscar preservar as informações, são:

I - Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

II - Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação;

III - Apoiar a implantação das iniciativas relativas à Segurança da Informação;

IV - Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

V - Criar e instituir controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação;

VI - Contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da infor garantias fundamentais.

Seção III

Dos perfis

Art. 7º. Os papéis e perfis a serem executados no PCSI/IPERON consistem na definição contida na Tabela 1:

Tabela 1: Descrição de papéis em Segurança da Informação

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	I - Servidores Públicos efetivos e comissionados; II - Estagiários, demais funcionários e colaboradores internos.	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do IPERON.
USUÁRIO EXTERNO	I - Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pela IPERON e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
GESTORES	I - Coordenadores; II - Diretores; III - Gerentes e demais cargos de chefia.	Todos aqueles que exercem funções de chefia no âmbito do IPERON, administrando pessoas e/ou processos.

ÁREA DE TIC	I – Servidores lotados no setor de TI do instituto.	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custo diante da informação.

CAPÍTULO V
DAS RESPONSABILIDADES

Seção I
Das responsabilidades Gerais

Art. 8º. As responsabilidades gerais na PCSI/IPERON são de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do IPERON e incluem:

I - Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

II - Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do Instituto;

III - Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do IPERON;

IV - Manter-se atualizado em relação a esta PCSI e às normas e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação da Instituição sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

Seção II
Responsabilidades Específicas

Art. 9º. As responsabilidades específicas são definidas de acordo com o perfil estabelecido, nos seguintes termos:

I - Usuários internos e externos: Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao IPERON em decorrência da não obediência às diretrizes e normas referidas na PCSI/IPERON e nas normas e procedimentos específicos dela decorrentes.

II - Gestores de pessoas e processos: Os gestores executivos do IPERON devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão.

§1º. Os usuários externos descritos no inciso I devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes;

§2º. O IPERON poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da PCSI/IPERON ou das normas e procedimentos específicos dela decorrentes.

Art. 10. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do IPERON, tomando as ações necessárias para cumprir tal responsabilidade.

Art. 11. Os Gestores e usuários da Área de Tecnologia da Informação deverão:

I - Zelar pela eficácia dos controles de Sistemas da Informação utilizados e informar aos gestores e demais interessados os riscos residuais;

II - Negociar e acordar com os gestores níveis de serviço relacionados a Sistemas da Informação, incluindo os procedimentos de resposta a incidentes;

III - Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

IV - Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

V - Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

VI - Informar previamente ao Gestor de Sistemas da Informação sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante;

VII - Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a uma pessoa física identificável como responsável pelo uso da conta (a responsabilidade pela gestão dos logins de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades);

VIII - Proteger continuamente todos os ativos de informação do Instituto contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código mal-intencionado e/ou indesejado;

IX - Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do IPERON ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas (quando tais ambientes forem acessados por terceiros, a responsabilização deve ser explicitada nas cláusulas dos instrumentos contratuais);

X - Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa, exigindo o seu cumprimento dentro da Autarquia;

XI - Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do IPERON, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do instituto.

CAPÍTULO VI
DAS DIRETRIZES

Seção I
Das Diretrizes Gerais

Art. 12. Ficam definidas as diretrizes específicas e procedimentos próprios de tratamento da informação corporativa, as quais adotarão as seguintes diretrizes gerais:

I - A informação utilizada pelo IPERON é um bem que tem valor que deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;

II - Deverão ser salvos em drives de rede, os documentos imprescindíveis para as atividades dos usuários da Instituição, os quais se gravados apenas localmente nos computadores, não terão garantia de backup e

poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

III - Arquivos pessoais e/ou não pertinentes às atividades institucionais do IPERON (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores.

IV - Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação dessa Norma;

V - O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível, o qual acontece através da identificação e autenticação do usuário;

VI - O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não devem ser utilizados para testes.

VII - A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse recinto para sua execução;

VIII - Todos os procedimentos que possibilitam a proteção da informação e a continuidade de seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos;

IX - Devem ser estabelecidos critérios para descarte seguro de informações armazenadas em estações de trabalho e/ou outros dispositivos de armazenamento, como formatação de máquinas ou desmagnetização de discos, quando o equipamento for transferido para outro usuário ou descartado pelo IPERON para algum outro destino;

X - O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação;

XI - A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas, as quais não estando ao alcance do Órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento;

XII - Toda informação crítica para o funcionamento do IPERON deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada;

§1º. Caso identificada a ocorrência disposta no inciso III, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário;

§2º. Os testes a que se refere o inciso VI, deverá ser feito em recinto apropriado e gerenciado;

§3º. O Gestor da Informação é responsável pela definição da criticidade descrita no inciso XII.

Seção II

Das Diretrizes Específicas

Art. 13. Fica estabelecido controle de acesso físico, lógico e procedimentos de contingências no ambiente computacional do IPERON, cujas diretrizes específicas são a seguir estabelecidas:

I - Dos Controles de Acesso Físico:

a) Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos do IPERON e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

b) Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado;

c) No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los;

d) Todo o pessoal envolvido em trabalhos de apoio tais como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

e) Todas as pessoas devem portar algum tipo de identificação visível que informe se é um servidor ou não, bem como o nível de autorização de acesso;

f) O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável;

g) O acesso ao Data Center somente será feito por servidores autorizados e com acompanhamento da equipe de TI do IPERON;

h) O Controle de acesso ao ambiente de DataCenter do IPERON será realizado preferencialmente com a instalação de fechadura biométrica;

e) Em caso da impossibilidade do acesso ao DataCenter ser realizado através de fechadura biométrica, é obrigatório o acompanhamento por servidor da área de TI do instituto;

II - Dos Controles de Acesso Lógico:

a) Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;

b) Os trechos que abrigam meios de comunicação devem ser protegidos para evitar a interceptação e/ou interferência de dados;

c) Os computadores e sistemas do IPERON devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados;

d) O responsável pela autorização ou confirmação da autorização a que se refere a alínea anterior deve ser claramente definido e registrado;

e) Os sistemas devem ser avaliados com relação aos aspectos de segurança antes de serem disponibilizados para a produção;

f) As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

g) O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

f) A equipe de TI do instituto poderá ter permissão de acesso remoto às estações de trabalho dos usuários das unidades quando necessário.

III – Procedimentos de Contingência e Backup:

1 - Os arquivos com conteúdo de grande importância cuja perda represente prejuízo para o IPERON, serão submetidos a uma rotina de backup periódico, preferencialmente de forma automática, mantendo-se no mínimo uma cópia em um servidor de backup.

2 - Documentos imprescindíveis para as atividades corporativas dos usuários deverão ser armazenados nos servidores da rede (Pasta Compartilhada), não sendo considerados para fins de backup os arquivos armazenados em estações de trabalho.

3 - Será implementada e disposta em manual específico, uma Política de Backup, realizada por um processo contínuo, definido de maneira formal, aplicado na implementação proteger as informações da rede contra a perda e/ou roubo de dados por meio de cópias de segurança das informações.

4 - O setor de TI do instituto implementará também, preferencialmente de forma automatizada, rotinas de backup dos bancos de dados e aplicações importantes utilizadas pelo IPERON.

5 - Será implementado e disposto em manual específico, rotinas de contingências para os riscos inerentes às atividades de tecnologia, entre elas: Falta de energia e Refrigeração no DataCenter, Falhas de Sistemas, Ataques Cibernéticos entre outros.

IV – Gestão da Segurança da Informação:

a) A gestão da segurança da informação será realizada pela **Diretoria de Tecnologia da informação** com apoio de todos os setores do instituto e terá responsabilidade de:

I - Prover todas as informações de Gestão de Segurança da Informação solicitadas pela Diretoria Executiva;

II - Prover ampla divulgação da Política e das Normas de Segurança;

III - Promover ações de conscientização sobre Segurança da Informação;

IV - Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação;

V- Elaborar e manter política de classificação da informação, com temporalidade para guarda;

VI – Definir procedimentos para auditoria de acesso e rotinas de recuperação de desastres;

Art. 14. Ficam estabelecidos critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação do IPERON, assim como estabelecidos critérios relativos às senhas das respectivas contas, devendo obedecer às disposições a seguir estabelecidas:

I - O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação do IPERON;

II - A criação e administração de contas serão realizadas de acordo com procedimento específico para todo e qualquer usuário;

III - Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível;

IV - Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

V - O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica;

Art. 15. Todas as estações de trabalho do IPERON devem estar adicionadas na ferramenta de gerenciamento de usuários de rede (AD – Active Directory).

Art. 16. Quando da criação da Conta de Acesso deverão ser observado os seguintes critérios:

I - Todo cadastramento de conta de acesso à rede do IPERON deve ser efetuado mediante solicitação formal;

II - Contas de acesso de terceirizados do IPERON devem ter prazo de validade no máximo igual ao período de vigência do contrato ou período de duração de suas atividades;

III - As solicitações relativas à criação de cada conta devem ser registradas e armazenadas de forma segura pela COOSIST/IPERON;

IV - Todos os usuários devem assinar Termo de Responsabilidade pela utilização da conta de acesso, ao qual deverá ser entregue junto com a solicitação de criação da conta de acesso;

V - A nomenclatura das contas de acesso de usuários deve seguir padrão definido pelo setor de TI do instituto;

VI - A chefia imediata da área a qual pertence o usuário deve ser informada formalmente, pelo setor de TI do instituto, a respeito de qualquer evento relacionado a falhas de segurança referente à conta do usuário e senha;

VII - Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicado ao setor de TI do instituto;

VIII - A conta de acesso é o instrumento para identificação do usuário na rede de dados do IPERON e caracteriza-se por ser de uso individual e intransferível, vedando-se sua divulgação em qualquer hipótese;

IX - A solicitação de criação de conta de acesso de usuário aos serviços de rede de dados do IPERON será feita pelo chefe imediato, via chamado registrado no “Sistema de Chamados do IPERON”. Somente em casos excepcionais, poderá ser enviado email para dtic@iperon.ro.gov.br.

X - O chamado para criação de conta de acesso deverá conter no mínimo o Nome do usuário, CPF, matricula, Setor de lotação e quais serviços serão necessário (rede local, pasta compartilhada, correio eletrônico).

Art. 17. Para exclusão e bloqueio da Conta de Acesso, serão observadas as seguintes disposições:

I - Toda exclusão ou bloqueio de conta de acesso à rede do IPERON deve ser efetuado mediante solicitação formal;

II - Contas sem utilização por mais de 45 (quarenta e cinco) dias serão bloqueadas pela equipe de TI do instituto;

III - As contas deverão permanecer bloqueadas até que haja nova solicitação formal para desbloqueio;

IV - As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de login/acesso;

V - As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos;

VI - As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva;

VII - Quando da mudança de setor ou exoneração, o chefe imediato deverá comunicar o setor de TI do instituto, via “Sistema de Chamados do IPERON” para que o remanejamento ou bloqueio do usuário seja realizado. Somente em casos excepcionais, poderá ser enviado email para dtic@iperon.ro.gov.br.

Parágrafo único. A exclusão da conta de acesso do usuário, prevista no inciso I deste artigo, deve ser solicitada nos seguintes casos:

I - Falecimento;

II - Aposentadoria; e

III - Outros afastamentos que caracterizem encerramento do vínculo com a instituição.

Art. 18. Todas as senhas, de usuários comuns, para autenticação na rede do IPERON devem seguir os seguintes critérios mínimos:

I - Toda senha deve ser constituída de, no mínimo, 7 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números);

II - São recomendados para uso em senhas:

1 - Caracteres alfanuméricos, por exemplo: “Ro253O4”;
2 - Caracteres mistos com maiúsculas e minúsculas, a exemplo de “IpSTmya”;
3 - Caracteres especiais, como “#”, “@”, “$”, “%”, “&”, “!”, “*”, “?”, “_”, “/”, “>”: “,”; “{“, “]”, “=”, “+”.

III - Não é considerado uma boa prática, a criação de senhas com:

1 - O mesmo nome do login de usuário para senha, por exemplo: Usuário: “maria”, Senha: “maria”;

2 - O nome do usuário ou combinações deste;

3 - Nomes de familiares, animais de estimação, datas de aniversário ou número de telefone;

4 - Nome de clubes de esportes;

5 - Repetição de números e/ou letras, por exemplo: “111111”, “aaabbb

IV - Não deverão ser reveladas senhas para colegas de trabalho, nem mesmo quando o servidor estiver em férias ou licença.

V - A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;

VI - É obrigatória a troca de senha ao efetuar o primeiro login;

VII - É proibida a repetição das 5 últimas senhas já utilizadas;

VIII - Os critérios definidos acima serão auditados pela equipe de TI do instituto, por meio de ferramentas adequadas;

IX - A base de dados de senhas deve ser armazenada com criptografia;

X - O usuário poderá solicitar alteração de sua senha, caso não se recorde da mesma, mediante solicitação formal;

§1º. A conta de acesso é o instrumento para identificação do usuário na rede IPERON e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese;

§2º. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário, ao qual as informações estão vinculadas;

§3º. A Gerência de Recursos Humanos do IPERON deve comunicar à equipe de TI do instituto, no prazo de dois dias úteis, os desligamentos, as aposentadorias, os afastamentos, licenças e as movimentações de usuários que impliquem mudanças de lotação;

§4º. O acesso aos serviços de tecnologia de informação do IPERON deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do IPERON;

§5º. Para fins de auditoria, as contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas pelos servidores da equipe de TI do instituto, quando estritamente necessário.

Art. 19. Fica instituído aos colaboradores do IPERON, os serviços de correio eletrônico (e-mail), observando-se os seguintes preceitos:

I - O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do IPERON, independentemente de seu vínculo funcional;

II - O correio eletrônico corporativo oficial do IPERON é unicamente aquele de domínio "@iperon.ro.gov.br", com exclusão de qualquer outro, não sendo aceitas como oficiais mensagens enviadas por domínio diverso.

III - O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do IPERON;

IV - São usuários do serviço de correio eletrônico corporativo os membros e servidores do IPERON, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do IPERON;

V - A concessão de contas de correio eletrônico depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade, para a Instituição, da utilização do serviço pelo agente;

VI - Os titulares de órgão ou unidade do IPERON podem solicitar a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

VII - Cada unidade do IPERON manterá no mínimo uma conta de correio eletrônico, destinada a comunicações institucionais;

VIII - É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

IX - O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico corporativo do IPERON, ou contidas em seus ambientes, será punido na forma da Lei;

X - O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

XI – O bloqueio/exclusão da conta de acesso ao email institucional, prevista no inciso I deste artigo, deve ser solicitada pelo setor de RH do instituto nos seguintes casos:

I - Falecimento;

II - Aposentadoria;

III - Licenças e;

III - Outros afastamentos que caracterizem encerramento do vínculo com a instituição.

Parágrafo único. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I - Praticar crimes e infrações de qualquer natureza;

II - Executar ações nocivas contra outros recursos computacionais do IPERON ou de redes externas;

III - Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

IV - Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do IPERON;

V- Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

VI - Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pelo IPERON;

VII - Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

VIII - Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

IX - Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

X - Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPERON ou suas unidades vulneráveis a ações civis ou criminais;

XI - Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

XI - Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

XIII - Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do IPERON estiver sujeita a algum tipo de investigação;

XIV - Fornecer orientação que conflite ou contrarie os interesses do IPERON;

XV - Disseminar ameaças eletrônicas, como: spam, mail bombing, vírus de computador; · . Distribuir ou fazer uso de arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

XVI - Obter acesso não autorizado a outro computador, servidor ou rede;

XVII - Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

XVIII - Burlar qualquer sistema de segurança;

XIX - Vigiar secretamente ou assediar outro usuário;

XX - Acessar informações confidenciais sem explícita autorização do proprietário;

XXI - Acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

XXII - Incluir imagens criptografadas ou de qualquer forma mascaradas;

XXIII - Distribuir conteúdo considerado impróprio, obsceno ou ilegal, de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

XXIV - Distribuir conteúdo de perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

XXV - Distribuir conteúdo que tenha fins políticos locais ou do país (propaganda política);

XXVI - Incluir material protegido por direitos autorais sem a permissão do detentor dos direitos;

XXVII - Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

Art. 20. Ficam estabelecidos procedimentos de controle de uso e acesso à Internet no âmbito do IPERON:

I - Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional;

II - Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do IPERON deverá sempre ser privilegiada;

III - Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos efetivos.

IV - Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o IPERON, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores;

V - Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando a assegurar o cumprimento da PCSI/IPERON;

VI - A instalação de softwares, inclusive navegadores e outros sistemas relacionados à internet, nos equipamentos computacionais do IPERON será feita apenas pelo setor de TI do instituto, vedada a instalação pelo usuário.

VII - É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Parágrafo único. São consideradas práticas inaceitáveis de acesso à internet, não se restringindo a estas:

I – Elaborar, utilizar, propagar, acessar ou de qualquer maneira manusear material de propaganda política, racismo, terrorismo, hacker, assédio sexual, pornografia, pedofilia, incentivo a violência, discriminação e outros não condizentes com os objetivos de trabalho corporativo, as leis vigentes e a ética;

II - Acessar ou fazer uso de sites de proxy online;

III - Acessar ou fazer uso de quaisquer tipos de jogos, inclusive online;

IV - Cessar ou fazer uso de programas que implementem usuário atua como servidor;

V - Acessar ou fazer uso de web rádio e web TV (sessões de transmissão contínua de vídeo e áudio);

VI - Acessar ou fazer uso de sites de conversação (bate-papo) e redes sociais;

VII - Baixar arquivos (downloads) ou executar arquivos do tipo “.exe”, “.dat”, “.sys”, “.bat” e outros tipos de arquivos executáveis;

VIII - Distribuir software ou conteúdo não autorizado (“pirataria”);

IX - Disseminar vírus, worms, cavalos de tróia ou qualquer outro tipo de código malicioso.

X – Fazer uso de programas que permitem compartilhar a internet do computador através de placa wireless, conhecido com o “Virtual Router”.

XI - Havendo instalação de softwares e sistemas nos equipamentos computacionais do IPERON, sem autorização e/ou licença devida, o usuário se tornará o responsável exclusivo utilização, arcando com eventuais penalidades e multas de acordo com a legislação vigente.

CAPÍTULO VII
DAS REGRAS PARA UTILIZAÇÃO DO SERVIÇO DE ACESSO REMOTO EXTERNO

Art. 21. As regras para utilização do serviço de acesso remoto externo à rede de dados do IPERON visam à prevenção do acesso não autorizado às informações, evitando ameaça sigilo das informações contidas na rede.

Art. 22. O acesso remoto externo à rede de dados do IPERON e a seus serviços corporativos somente será disponibilizado aos usuários que, oficialmente, executem atividade vinculada à atuação governamental e necessitam daquele acesso para execução de atividades externas, desde que devidamente autorizados pelo chefe imediato e certificados pela Equipe de Ti do IPERON.

Art. 23. É vedada a utilização do acesso remoto para fins não relacionados às atividades corporativas.

Art. 24. A Equipe de TI do IPERON irá monitorar e registrar toda conexão remota e de acesso à sua rede de dados.

Art. 25. Os administradores de redes poderão ter permissão de acesso remoto aos recursos de TIC do IPERON, quando necessário para o desempenho de suas atribuições.

Art. 26. A solicitação de acesso remoto ocorrerá por meio de chamado registrado no sistema de chamados do instituto, contendo as seguintes informações do usuário e do serviço: nome completo, CPF, Matrícula, setor, e-mail e telefone de contato, IP de destino, porta do serviço e Justificativa.

Art. 27. O serviço de acesso remoto será cancelado nas seguintes condições:

1 - Finalização do período especificado na solicitação;

2 - Perda da necessidade de utilização do serviço;

3 - Transferência ou exoneração do usuário;

4 - Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

CAPÍTULO VII
DA SEGURANÇA NAS COMUNICAÇÕES

Art. 28. A rede de dados do IPERON utilizará serviços de controle de fluxo de filtrar e ordenar todas as informações transitadas e garantir sua proteção.

§1º A equipe de TI do IPERON manterá e administrará firewalls em todos os segmentos da rede, gerenciando todo o tráfego de entrada e saída;

§2º Um firewall é uma passagem (“gateway”), também conhecido como “proteção de borda”, que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a internet e pode também estabelecer passagens seguras entre redes internas;

§3º Para manter o controle na entrada e saída de informações da rede, qualquer autorização ou bloqueio nos controles de fluxo de dados deverá ocorrer por meio de chamado no “Sistema de Chamados do IPERON”;

§4º Todo ativo de rede na rede de dados do IPERON, exceto as estações de trabalho, deverá ser monitorado pela equipe de TI, tanto nas interfaces onde transitam as informações quanto em seus componentes de hardware, com ferramentas adquiridas para tal fim;

CAPÍTULO VIII
DO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Art. 29. Todo desenvolvimento ou manutenção de sistemas deve ser precedido por uma análise de impacto e ser formalmente autorizado pelo chefe imediato do setor de desenvolvimento.

Art. 30. Toda alteração de escopo de desenvolvimento ou documentada e formalmente autorizada pelo chefe imediato.

Art. 31. Os requisitos ou funcionalidades de domínio devem ser especificados e documentados juntamente com um representante do sistema, bem como as manutenções necessárias, considerando os requisitos de segurança definidos no desenvolvimento do sistema.

Art. 32. Todo sistema que implique manipulação de dados deve ser desenvolvido de acordo com as regras de controle de acesso a informações de natureza restrita ou sigilosa.

Parágrafo único. Em caso de manipulação de dados sensíveis, mecanismos adicionais que possibilitem a rastreabilidade das operações efetuadas devem ser considerados.

Art. 33. Os ambientes de desenvolvimento de testes, de homologação e de produção serão isolados entre si.

Art. 34. Devem ser definidos e utilizados procedimentos de testes no sistema para todo desenvolvimento ou manutenção realizados, os quais devem contemplar controles a seguir destacados:

I - validação de dados de entrada;

II - controle de processamento interno;

III - integridade de mensagens;

IV - validação de dados de saída;

V- Testes automatizados;

VI - Testes de carga;

VII. Testes de estresse.

Parágrafo único. Poderão ser utilizados outros controles diversos dos previstos nos incisos deste artigo a critério da administração.

Art. 35. Será estabelecida uma metodologia para todo desenvolvimento ou manutenção, com base nas melhores práticas de mercado que deverá contemplar as seguintes fases:

I - Planejamento;

II - análise de requisitos;

III - Projeto;

IV - Codificação;

V - Revisão;

VI - Compilação e testes.

Parágrafo único. Poderão ser utilizados e/ou acrescentadas outras fases diversas das previstos nos incisos deste artigo a critério da administração.

CAPÍTULO IX
DAS PENALIDADES

Art. 36. O não cumprimento das determinações ora apresentadas sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do IPERON.

§ 1º. O descumprimento das disposições constantes nessa PCSI/IPERON sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

§ 2º. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei Complementar nº 68/92 e demais legislação pertinente;

CAPÍTULO X
DA ATUALIZAÇÃO

Art. 37. Esse PCSI/IPERON deve ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 38. As informações produzidas por usuários do IPERON e não cabe a seus criadores qualquer forma de direito autoral.

§ 1º. Quando as informações forem produzidas por terceiros para uso exclusivo do IPERON, instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

§ 2º. É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo IPERON, salvo autorização específica pela Presidência, nos processos e documentos de sua competência e demais casos.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 39. Para a uniformização da informação organizacional, esta PCSI/ IPERON deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do IPERON – a fim de que seja

cumprida dentro e fora da autarquia.

Art. 40. O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

Art. 41. A presente Política tem como fundamentos as seguintes referências legais e normativas:

I - Lei Federal nº 13.709, de 14 de agosto de 2018 Pessoais (LGPD);

II. Lei Federal nº 12.965, de 23 de abril de 2014

III. Lei Federal nº 12.527, de 18 de novembro de 2011

IV. Decreto Federal nº 9.637 de 26 de dezembro de 2018 Segurança da Informação, dispõe sobre a governança da segurança da informação;

V. Lei Complementar Estadual nº 68, de 09 de dezembro de 1992 Regime Jurídico dos Servidores Públicos

VI. Decreto Estadual nº 9.832 de 12 de junho de 2019 Segurança da Informação;

VII. NBR/ISO/IEC 27001/2006 Segurança da Informação;

VIII. NBR/ISO/IEC 27002/2013 Segurança da Informação;

IX. NBR/ISO/IEC 27005:2008 da Informação;

X. Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, man com inteiro teor em http://cartilha.cert.br;

XI. Portaria nº 97 de 09 de junho de 2021 – Política de Segurança da Informação SETIC.

Art. 42. Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos à Procuradoria Geral e Presidência do IPERON;

Art. 43. Esta Resolução entra em vigor na data de sua publicação.

ANEXO I
POLÍTICA DE MESA LIMPA E POLÍTICA DE TELA LIMPA

1 - Este Anexo institui a política de mesa limpa para papéis e mídias removíveis, bem como a política de tela limpa para os recursos de processamento da informação, reduzindo assim os riscos de acessos não autorizados, danos e perdas de informações durante e fora do horário normal de trabalho.

2 - Esta política deverá considerar a classificação das informações, os riscos correspondentes e os aspectos culturais do IPERON.

3 - Os servidores deverão observar que os documentos, dispositivos e quaisquer informações deixadas sobre as mesas de trabalho são potenciais alvos para furtos, ou mesmo, podem ser extraviadas. Da mesma forma, essas fontes de informação, caso deixadas sobre as mesas, estarão expostas ao risco de danos ou destruição em caso de sinistro, como incêndios ou inundações por exemplo.

4 - Os pontos de controle recomendados são os listados abaixo:

a) Papéis e mídias de computador, quando não estiverem sendo utilizados, devem ser guardados em locais seguros (cofres, arquivos metálicos ou gavetas), com fechaduras, principalmente fora do horário de expediente normal.

b) Informações restritas ou sigilosas, quando não requeridas, devem ser guardadas em local distante, seguro e fechado, se possível em um cofre ou arquivo resistente a incêndios, principalmente após o expediente ou quando o local de trabalho estiver vazio.

c) Computadores pessoais, estações de trabalho e impressoras não devem ser deixados ligados quando não assistidos, e sempre devem estar protegidos por senhas, chaves ou outros tipos de controle de acesso.

d) Área de Trabalho ou Desktop nas estações de trabalho não devem ser local de armazenamento de informações. As Informações deverão ser mantidas nos de rede e/ou nuvem.

Uma política de mesa e tela limpa reduz o risco de acesso não autorizado, perda e dano de informações durante e após o horário normal de trabalho. Cofres, servidores de rede e outras formas de instalações de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

Maria Rejane Sampaio dos Santos Vieira

Presidente/IPERON

Documento assinado eletronicamente por **Maria Rejane Sampaio dos Santos Vieira**, **Presidente**, em 06/04/2022, às 11:22, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0027852034** e o código CRC **DCDCD5EF**.

Referência: Caso responda esta Resolução, indicar expressamente o Processo nº 0016.068599/2022-23 SEI nº 0027852034