POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

A informação é um dos principais patrimônios no mundo corporativo. Um fluxo de informação de qualidade é capaz de decidir o sucesso ou fracasso na tomada de decisões de uma organização, seja pública ou privada. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos e prejudicar a imagem de qualquer instituição perante a sociedade. Atento a isso, o IGEPPS divulga ao seu corpo técnico sua Política de Segurança da Informação, o alicerce dos esforços de proteção à informação, aplicados a sua infraestrutura operacional.

OBJETIVO

Esta Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificulte o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados;
- O seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores em todo o processo.

Diante do exposto, este documento ***- Política da Segurança da Informação -*** vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: continuidade de sua área fim e aplicar segurança a este.

Para a manutenção deste documento em conformidade com a legislação vigente, é importante que o mesmo seja revisto periodicamente, com vista a sua adequação tecnológica e legal.

ABRANGÊNCIA

Esta Política de Segurança se aplica a todos os servidores públicos lotados nesta autarquia – efetivos, temporários, comissionados ou cedidos de outros órgãos (autarquias ou secretarias do Estado do Pará) – estendendo-se ao corpo técnico de fornecedores a serviço do IGEPPS.

CONCEITOS E DEFINIÇÕES

São identificados como recursos de infraestrutura tecnológica do IGEPPS: os microcomputadores, os nobreaks, as redes de comunicação de dados e voz, periféricos associados aos computadores (teclado e mouse), as câmeras de monitoramento e os equipamentos de controle de acesso, equipamentos de projeção e painel de chamadas, softwares disponibilizados pelo IGEPPS para a execução das atividades laborais de seus servidores:

Segurança da Informação se entende como o esforço contínuo em proteger e preservar os ativos computacionais, visando atender os preceitos da Confidencialidade, Integridade e Disponibilidade.

Para tal é necessário preservar e assimilar conceitos inerentes ao assunto:

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, assim como utilizar os recursos computacionais de um órgão e/ou empresa.

Autenticidade: garantir que a informação é proveniente da fonte anunciada e que não foi alvo de alterações ao longo do processo.

Confidencialidade: garantia que a informação é acessível somente as pessoas autorizadas, pelo período necessário e para os fins de atividade relacionados a sua função.

Comitê Gestor de Segurança da Informação: grupo multidisciplinar composto por membros do corpo técnico e estratégico, com objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pelo IGEPPS.

Disponibilidade: garantir que a informação ou dado estará acessível para as pessoas autorizadas sempre que for necessário.

Integridade: Garantia que a informação esteja completa e integra, não tendo sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

Informação: Conjunto de dados, textos, imagens, sistemas ou outra forma de representação datada de significado em determinado contexto, independente do suporte em que resida ou esteja armazenada.

Usuário Interno: Empregado, servidor, contratado, estagiário ou comissionado ligado a Administração Pública Estadual que no exercício de suas funções, tenham acesso a informações produzidas ou recebidas por esta autarquia.

Usuário Externo: a pessoa física ou pessoa jurídica que tenha acesso concedido a informações produzidas ou recebidas pelo IGEPPS e que não tenho vínculo direto a esta autarquia ou outro órgão da gestão administrativa estadual.

PREMISSAS / DIRETRIZES

*Informação é **PATRIMÔNIO***
As informações geradas, adquiridas e/ou custodiadas pelo IGEPPS são consideradas parte do patrimônio e devem ter os atributos de confidencialidade, integridade e disponibilidade garantidos.

Acesso Restrito e Controlado
A autorização, o acesso e o uso da informação e de seus recursos devem ser controlados e limitados as atividades profissionais necessárias ao cumprimento das funções de cada colaborador, tais como sistemas de informação, internet, e-mail e rede de comunicação.

Utilização dos recursos computacionais
Apenas equipamentos e softwares disponibilizados e homologados pela CTIN/IGEPPS serão autorizados a ser instalados e conectados à rede de dados corporativa.

Equipamentos particulares
O uso de qualquer equipamento particular, seja computador ou dispositivo portátil capaz de armazenar e/ou processar dados, será desautorizado a ingressar ou ter acesso a rede de dados do IGEPPS.

Área de Trabalho
Nenhuma informação confidencial deve ser deixada a vista, seja este documento físico ou virtual – através de dispositivo eletrônico autorizado.

Recursos Compartilhados
Certifique-se do acesso autorizado ao recurso computacional e tenha ciência do uso consciente deste.

Postura profissional
Evite discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mídias sociais, evitando expor a imagem desta autarquia.

Todos são responsáveis pela Segurança
Todo servidor é responsável pela segurança das informações, ativos e processos que estejam sob sua custodia e por todos os atos executados com suas identificações. Qualquer que seja a forma de identificação, ela deve ser pessoal e intransferível, permitido, de maneira clara e indiscutível, o reconhecimento de qualquer usuário.

Educação é fundamental para Segurança
O conteúdo desta politica e demais normas que a apoiam tem que ser conhecido e cumprido por todos os colaboradores, que devem, obrigatoriamente, notificar, de forma exclusiva e imediata, os responsáveis em casos de suspeita ou violação das regras e falha na segurança da informação.

As informações devem ser Classificadas
Toda informação deve ser classificada quanto a sua confidencialidade, integridade e disponibilidade e receber tratamento adequado.

Direitos de Propriedade

Todo produto resultante do trabalho do servidor (coleta de dados e documentos, sistema, processos e outros) é de propriedade do IGEPPS.

Gestão de Riscos de Segurança e Continuidade dos Negócios

As informações classificadas como críticas e vitais para o negócio do IGEPPS, bem como os ativos que as suportam, devem ter seus riscos identificados, mitigados e receber tratamento adequado quanto a sua disponibilidade. Todos os incidentes que comprometam a Segurança da Informação, inclusive na rede de comunicação de dados, devem ser registrados e tratados de forma tempestiva.

Informação e fornecedores

Nas relações com terceiros em que haja a necessidade de troca de informações entre instituições, o sigilo deverá ser garantido, quando for o caso, por meio de termos de confidencialidade ou clausula que trate desta proteção.

Verificação de Controles

Os controles definidos a partir destas diretrizes devem ser normatizados e verificados periodicamente quanto ao seu cumprimento e necessidade de adequação, pela área de Segurança da Informação.

RESPONSABILIDADES

Dos usuários autorizados:

- Cumprimento da Política de Segurança da Informação.
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho.
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso.
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.
- Assegurar que as informações e dados de propriedade do **IGEPPS** não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
- Relatar para o seu responsável hierárquico e à Coordenação da **CTIN**, o surgimento da necessidade de um novo software para suas atividades.
- Responder pelo prejuízo ou dano que vier a provocar ao **IGEPPS** ou a terceiros, em decorrência da não obediência as recomendações gerais definidas em documento anexo.

Dos Superiores Hierárquicos:

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação.
- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão.

- Autorizar o acesso e definir o perfil do usuário junto a **CTIN** através das ferramentas de colaboração disponibilizadas ao corpo funcional do **IGEPPS**.
- Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI.
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação.
- Notificar imediatamente ao gestor da **CTIN** quaisquer vulnerabilidades e ameaças a quebra de segurança.
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação.
- Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato à **CTIN**.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Da Gestão de Pessoas:

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação.
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI do **IGEPPS**.
- Exigir de fornecedores, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Informar, sempre que necessário, atualizações referentes a cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade.
- Tomar as decisões administrativas referentes aos descumprimentos da PSI do **IGEPPS**.

Da CTIN

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação.
- Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Restringir o acesso ao ambiente computacional sob sua responsabilidade a pessoal não autorizado.
- Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio.
- Gerenciar o descarte de informações a pedido.
- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários garantindo a segurança por área do negócio.
- Criar a identidade lógica dos colaboradores na empresa.

- Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas e qualquer outro ativo de informação.
- Proteger todos os ativos de informação do **IGEPPS** contra códigos maliciosos e ou vírus.
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro do **IGEPPS**.
- Realizar inspeções periódicas de configurações técnicas e análise de riscos.
- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais.
- Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento do **IGEPPS** ou parceiro autorizado.
- Propor as metodologias, sistemas e processos específicos que visem aumentar a segurança da informação.
- Promover a conscientização dos colaboradores em relação a relevância da segurança da informação.
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços.
- Buscar alinhamento com as diretrizes do **IGEPPS**.
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso a internet e aos sistemas críticos do **IGEPPS**, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos as redes externas, inclusive internet.
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação de gestor (ou superior), conforme procedimento publicado na matriz de responsabilidade.
- Realizar, a qualquer tempo, inspeção física nas máquinas instaladas nas dependências físicas do **IGEPPS**, inclusive, máquinas autorizadas de parceiros/fornecedores.

COMPETÊNCIAS

É de responsabilidade do ***Comitê Gestor de Segurança da Informação***, conselho representativo em face de estrutura organizacional atual, assegurar a aplicação das diretrizes e normas constantes na Política de Segurança da Informação através de ações e comunicados acessíveis a todos os servidores e colaboradores autorizados ao uso da infraestrutura computacional do IGEPPS.

VIOLAÇÃO E PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência verbal, advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar cabível ao assunto.

No caso da aplicação de advertência ao servidor e/ou colaborador infringindo o PSI, aplicar-se-á ações:

- Advertência verbal
    - O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação do IGEPPS e será recomendado à leitura da PSI e Normativas.
- Advertência formal
    - A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida.
    - A segunda notificação será encaminhada para a chefia imediata do infrator.

ATUALIZAÇÕES

O Comitê Gestor e a CTIN se reservam ao direito de revisar, adicionar ou modificar esta Política de Segurança da Informação para aprimorar e garantir o perfeito funcionamento das normas e regras por ele definidas, principalmente aos casos omissos, que deverão ser encaminhados a CTIN para avaliação e resolução com o Comitê Gestor.

As normas e procedimentos acima não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol taxativo, motivo pelo qual é obrigação do CGSI, bem como dos usuários adotarem todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações desta Autarquia.

CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à **CTIN**, que avaliará junto ao Comitê de Gestão de Segurança da Informação, esclarecendo formalmente ao setor solicitante.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão do Comitê Gestor de Segurança, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

Uso dos Recursos Computacionais – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1 Estabelecer critérios para o acesso e utilização dos recursos computacionais disponibilizados pelo IGEPPS – *hardware* ou *software*.

2. REGRA GERAL

2.1 Computadores e demais recursos desta Autarquia devem ser usados exclusivamente para o serviço do IGEPPS.

2.1.1 Uso particular dos recursos pode ser autorizado de forma esporádica, por meio de solicitação de superior hierárquico e autorização da CTIN.

2.1.2 O IGEPPS poderá realizar auditorias/perícia/investigação nos recursos computacionais disponibilizados, como, por exemplo, os computadores e/ou celulares corporativos, sempre que considerar necessário, ainda que sem aviso prévio, atendendo os princípios da proporcionalidade e razoabilidade.

2.1.3 O IGEPPS poderá ter acesso às informações de caráter pessoal de seus servidores, em razão da auditoria/perícia/investigação, se estes utilizarem os equipamentos institucionais indevidamente para armazenar seus dados pessoais.

2.2 Por se tratar do interesse comum desta Autarquia, todos os servidores do IGEPPS têm permissão para acessar portais de notícias que tratem de assuntos previdenciários, jurídicos governamentais, identificados em sua maioria pelos domínios ADV.BR e GOV.BR.

2.2.1 Domínios de exceção serão tratados pontualmente.

2.3 Equipamentos devem ser manuseados com atenção, devendo considerar que se trata de patrimônio do IGEPPS.

2.3.1 Em caso de anormalidade destes informar imediatamente a CTIN através do sistema de chamados GLPI.

2.3.2 Em caso de ausência ou desaparecimento de equipamento, deve-se avisar imediatamente a CTIN para que sejam tomadas as medidas cabíveis.

2.3.3 Evite o consumo de alimento ou bebida próximo da sua área de trabalho.

2.3.4 Não é permitida a abertura física ou desmontagem de equipamento por pessoa não autorizada, exceto se realizada por colaborador de empresa autorizada.

2.3.5 Em caso de roubo ou furto, o servidor deverá fazer o BO (Boletim de Ocorrência) e notificar a CTIN através do sistema de chamados GLPI, inserindo o número de BO e providenciando uma cópia para deixar no IGEPPS.

2.4 Mudança de local de equipamentos só serão realizadas pelo corpo técnico da CTIN, após avaliação lógica e elétrica do espaço fisco, com o objetivo de evitar danos ou acidentes.

2.4.1 Em caso de transferência de equipamento para outro setor, a ação será realizada após autorização de mudança entre coordenações envolvidas, movimentação patrimonial e avaliação lógica do espaço. Os setores CTIN e GSA deverão ser notificados por meio de registro de chamado no GLPI.

2.4.2 Nos casos de mudança de equipamento, o servidor deverá assinar o termo de devolução de ativo do sistema que estará entregando e o termo de recebimento do novo ativo.

2.5 O acesso às informações e uso de sistemas e aplicativos deverão ser feitos mediante identificação do usuário único, pessoal, e intransferível, com utilização do conjunto de acesso USUÁRIO e SENHA. O usuário é responsável pelas ações realizadas por meio de utilização de suas credenciais de acesso e é de sua responsabilidade o sigilo de suas senhas de acesso aos recursos computacionais disponibilizados.

2.6 O uso das informações, sistemas e aplicativos disponibilizados pelo IGEPPS é monitorado.

2.7 Não é permitida a instalação de equipamento ou *software* na rede corporativa do IGEPPS sem a prévia autorização da CTIN.

2.8 É expressamente proibido o envio de qualquer mensagem, seja entre os servidores do IGEPPS ou parceiros fornecedores, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, *bullying*, *SPAMS*, correntes ou qualquer natureza similar, indução religiosa, comércio, propaganda e incentivo a atos de terrorismo ou que visem instigar, ameaçar, invadir a privacidade ou prejudicar pessoas e/ou instituições.

2.8.1 É vedado uso de e-mail externo aos servidores desta Autarquia.

2.9 É expressamente proibido utilizar os recursos computacionais para executar fraudes ou ações de natureza similar.

2.10 É proibido fazer *download* e/ou armazenar em computador institucional ou unidade de rede: *software* comercial, músicas, imagens, filmes, vídeos ou qualquer outro material cujo direito pertença a terceiros (*copyright*) sem ter um contrato de licenciamento, compra ou outro tipo de licença, e programas ou arquivos de conteúdo pornográfico ou de qualquer outra natureza que não seja para fins relacionados às atividades da instituição.

2.11 O IGEPPS disponibiliza unidade de rede para armazenamento de informações institucionais que precisam ser protegidas. É de responsabilidade exclusiva do usuário manter na rede (servidor de arquivos) as informações produzidas a fim de facilitar as consultas pelos demais servidores e ações de segurança e prevenção a incidentes.

2.12. Arquivos de música, vídeo, jogos, fotos e outros não estão de acordo com os serviços realizados pelo IGEPPS, portanto, serão sumariamente excluídos assim que encontrados.

2.12.1. Caso seja encontrado *backup* de estação de trabalho e/ou de caixa postal do e-mail institucional, o usuário será notificado para o possível resgate do *backup* que posteriormente será extraído para análise pelo setor da CTIN.

2.12.2. O IGEPPS não é responsável por arquivos mantidos nas estações de trabalho, seja a natureza institucional ou pessoal.

2.12.3. O IGEPPS não inclui em sua política de *backup*, estação de trabalho de servidor(colaborador) algum.

2.13. Para fins de segurança institucional, estão bloqueados nas estações de trabalho desta Autarquia os acessos às unidades leitoras de mídias ópticas, as portas USB´s e as placas de rede wireless.

2.14. É terminantemente proibido fazer uso de serviços de armazenamento em nuvem para transferência ou backup de informações desta Autarquia que não sejam estabelecidos e disponibilizados pela instituição.

Identificação, controle e gestão – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1 Estabelecer critérios para a identificação do usuário da rede do IGEPPS, assim como a concessão dos acessos necessários ao desenvolvimento de suas atividades laborais, tal como a gestão de acessos.

2. DEFINIÇÃO

2.1 Entende-se por usuário: qualquer conta de usuário, devidamente cadastrada pela autarquia, com acesso aos sistemas/recursos computacionais do IGEPPS.

2.1.1 Classificamos como usuário externo, toda pessoa física ou jurídica prestadora de serviço que tenha acesso concedido às informações recebidas ou tratadas pelo IGEPPS.

2.1.2 Classificamos como usuário interno, todo indivíduo identificado nesta Autarquia como servidor efetivo, temporário, cedido, comissionado, contratado ou estagiário, que no exercício de suas funções tenham acesso a informações recebidas ou tratadas pelo IGEPPS.

2.1.3 Classificamos como usuário de sistema, as contas de usuários necessários que sejam criados para funcionar a comunicação entre um sistema, aplicação e banco de dados.

2.2 Entendem-se por contas temporárias aquelas que serão utilizadas por um período específico, por exemplo, para terceirizados em serviço para a Autarquia.

2.3 Contas de emergência, por sua vez, são criadas para situações de justificada urgência, como para atender demandas de órgãos fiscalizadores.

3. IDENTIFICAÇÃO DE ACESSO LOCAL

3.1 Cada usuário deve possuir conta única, pessoal e intrasferível para acesso à rede institucional e remota do IGEPPS.

3.2 A criação e o gerenciamento de conta de usuário, login de acesso a rede institucional e aos sistemas informatizados devem ser executadas pela CTIN, através de solicitação formal da Coordenação e Desenvolvimento de Pessoas (CODP) ou solicitação de acesso da Coordenadoria imediata do servidor.

3.3 Permissões devem ser concedidas de forma que o usuário tenha somente o acesso necessário para a execução de suas funções.

3.4 O usuário é responsável pelas atividades realizadas por meio da utilização de sua conta de acesso à rede institucional e as credenciais dos Sistemas Informatizados.

3.5 A senha associada a conta do usuário para acesso à rede institucional é pessoal, intransferível e o devido sigilo é de responsabilidade do usuário.

3.5.1 A CTIN é responsável pela definição e divulgação das regras de formação da senha associada.

3.5.2 É de responsabilidade da CODP comunicar o desligamento de servidores e estagiários, para que as permissões que foram concedidas sejam imediatamente revogadas.

3.5.3 É de responsabilidade das Coordenadorias gestoras de contratos de prestação de serviços terceirizados comunicar o desligamento de colaboradores ou fornecedores a serviço, para que as permissões do acesso sejam imediatamente revogadas.

3.5.4 É de reponsabilidade da CODP e Coordenadorias envolvidas, comunicar à CTIN, a transferência de servidores, estagiários para o devido ajuste de suas permissões de acesso.

3.6 Todas as senhas de acesso à rede institucional do IGEPPS devem seguir os seguintes critérios:

3.6.1 Toda senha deve ser constituída de, no mínimo, 10 caracteres sendo obrigatório o uso de caracteres minúsculos, maiúsculos, dígitos e caracteres especiais (como por exemplo: ponto, vírgula, hashtag);

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

3.6.3 Será obrigatória a troca de senha ao efetuar o primeiro *logon* na rede institucional;

3.6.4 Não será permitida a repetição das últimas 5 senhas já utilizadas.

3.7 A criação e manutenção de acessos emergenciais ou temporários deverão ser gerenciados pela CTIN, que também deverá revogá-los após exaurida a finalidade que os justificou.

3.8 Todas as solicitações devem ser formalizadas e transitadas no sistema de chamados da CTIN.

3.8.1 Endereço de acesso http://glpi.igeprev-pa.inst.prev.

3.9 Nos contratos estabelecidos com empresas terceirizadas deverão constar cláusulas de confidencialidade, bem como cláusulas que determinem a aderência à Política de Segurança da Informação do IGEPPS e as sanções cabíveis em caso de descumprimento.

3.10 A CTIN é responsável pelo monitoramento dos acessos concedidos assim como a sua revisão periódica ou sempre que necessário.

3.10.1 A base de dados de senhas deve ser armazenada com criptografia;

3.10.2 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. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos recursos computacionais.

3.11 Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

4. PARA ACESSO REMOTO

4.1 O acesso remoto aos serviços institucionais somente será disponibilizado aos servidores do IGEPPS que, oficialmente, executem atividades vinculadas à atuação institucional desta Autarquia.

4.1.1 O acesso deve ser solicitado pela Coordenadoria vinculada ao servidor, justificando a necessidade deste acesso e definindo a periodicidade.

4.1.2 A tramitação desta solicitação dar-se-á através do Sistemas de Chamados da CTIN e deverá ser autorizada pelo Gabinete da Presidência.

4.2 A liberação do acesso remoto só será efetivada após as autorizações gerenciais envolvidas com manifestação registrada no sistema de chamados GLPI, ficando sob responsabilidade da CTIN notificar ao servidor, sua liberação de acesso.

4.2.1 Será enviado para o e-mail do solicitante o manual de orientação para a configuração do acesso remoto privado e a customização de seu acesso à rede do IGEPPS.

4.2.2 A configuração de um dispositivo portátil ou computador de mesa pessoal é de responsabilidade do servidor autorizado, ficando a CTIN isenta de responsabilidade sobre a integridade dos sistemas instalados neste equipamento.

4.3 As conexões remotas da rede institucional do IGEPPS devem ocorrer da seguinte maneira:

4.3.1 Utilização de autenticação forte, como o uso de senhas complexas, descritas no item 3.6.1 desta normativa e, quando possível, o uso de multifator de autenticação;

4.3.2 As senhas e informações que trafegam entre a estação remota e a rede do IGEPPS devem ser criptografadas;

4.3.3 É vedada a utilização do acesso remoto para fins não relacionados às atividades do Instituto.

4.3.4 É vedada a utilização deste recurso a colaboradores sem vínculo institucional.

4.3.4.1 A exceção é aplicada aos fornecedores de Tecnologia da Informação mediante assinatura de Termo de Confidencialidade e cláusula explícita em Contrato de Prestação de Serviços.

4.4 O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

4.4.1 Finalização do período solicitado ou término do Contrato;

4.4.2 Perda de necessidade de utilização do serviço;

4.4.3 Transferência do usuário para outra secretaria ou Autarquia do Governo do Estado do Pará;

4.4.4 Identificação de vulnerabilidade, risco ou uso indevido;

4.4.5 Por ordem expressa do Presidente desta Autarquia.

Disponibilização e Gestão de Recursos Computacionais – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1 Estabelecer critérios para o acesso, utilização e gerenciamento de recursos computacionais disponibilizados na rede institucional do IGEPPS, assim como a responsabilização em caso de sinistro.

2. DEFINIÇÃO

2.1 Entende-se por **RECURSO COMPUTACIONAL** todo ativo (físico e lógico) ou serviço disponibilizado aos servidores ou fornecedores autorizados do IGEPPS.

2.2 Entende-se por **Endpoint** todo dispositivo de usuário na rede tratado como ponto de extremidade ou último dispositivo na rede.

3. ARMAZENAMENTO DE ARQUIVOS

3.1 A CTIN deve aplicar solução de segurança na rede institucional, a fim de prover ambiente seguro para o armazenamento de dados pessoais, sensíveis e confidenciais.

3.2 Diretorias, Coordenadorias e Gerências têm seu diretório de rede específico na rede.

3.2.1 As definições de acesso aos diretórios é responsabilidade da CTIN.

3.2.2 O Gestor deve solicitar à CTIN a concessão, a alteração ou a revogação de permissão sobre o diretório de sua sessão conforme a necessidade de sua equipe.

3.2.3 Caso seja necessário acesso a diretório de outra Coordenação, este deve ser autorizado e definido o tipo de acesso (**proprietário, editor e consultivo)** pelo Gestor do solicitante.

3.2.4 O item anterior não se aplica ao diretório da CTIN e diretório com conteúdo sigiloso, cuja responsabilidade é de responsabilidade da CTIN e Gabinete da Presidência, respectivamente.

3.3 É vedado o armazenamento das seguintes informações ou conteúdos nos diretórios da rede institucional do IGEPPS:

3.3.1 Arquivo em desacordo com a Política de Segurança da Informação ou de Privacidade do IGEPPS, tal como arquivos de imagens, vídeo, áudio e outros que não sejam do interesse do IGEPPS ou necessários à execução de atividades fim.

3.3.2 Programa não homologado ou licenciado pela CTIN.

3.3.3 Programa de conteúdo potencialmente prejudicial à segurança da rede institucional.

3.3.4 Programa em desacordo com critérios e requisitos de segurança de que trata a Política de Segurança do IGEPPS.

3.3.5 Cópia de segurança de diretório particular ou cópia-imagem de estação de trabalho. Destaca-se que o IGEPPS se exime de qualquer responsabilidade sobre dados armazenados em estações de trabalho.

3.4 As informações armazenadas na rede institucional serão inspecionadas pela CTIN periodicamente, através de ferramenta adequada à atividade. Mediante o indício de armazenamento de conteúdo não autorizado e em desacordo a esta normativa serão tomadas as seguintes ações:

3.4.1 Identificação do conteúdo;

3.4.2 Materialidade do conteúdo;

3.4.3 Remoção do conteúdo;

3.4.4 Registro do incidente no Sistema de Gerenciamento de Segurança da Informação;

3.4.5 Notificação do fato à Coordenação responsável pelo servidor.

4. DA INSTALAÇÃO E EXECUÇÃO DE PROGRAMAS

4.1 A instalação de programas em estações trabalho é de responsabilidade da CTIN e/ou fornecedor expressamente autorizado.

4.2 É vedado ao usuário desabilitar ou desinstalar programas de qualquer natureza nas estações de trabalho.

4.3 Cabe à CTIN manter atualizada e divulgar a relação de programas homologados e licenciados para utilização da rede institucional.

4.3.1 Todas as estações de trabalho deverão conter sistemas de segurança como o uso de antivírus e, caberá à CTIN:

4.3.1.1 Monitorar os *status* dos antivírus, identificando se houve alguma detecção de *malware* e verificar se todos os sistemas estão com as últimas atualizações instaladas;

4.3.1.2 Realizar as atualizações necessárias, sempre que preciso;

4.3.1.3 Instalar o antivírus mais adequado, bem como, se julgar necessário, tomar medidas proativas para combater/prevenir possíveis ameaças.

4.4 Cabe à CTIN configurar o uso de comunicação criptografada em todas as estações de trabalho que podem ser utilizadas fora do Instituto, como *laptops*, para fins institucionais. A CTIN é responsável por gerenciar as contas de usuários, a fim de garantir a disponibilidade dos ativos na hipótese de esquecimento de senhas ou de realização de auditorias e investigações internas ou externas decorrentes de incidentes de segurança da informação.

4.4.1 O Comitê Gestor de Segurança da Informação (CGSI) deverá ter acesso à gestão de chaves criptográficas e poderá solicitar a qualquer momento o acesso às contas e dispositivos do órgão, com o objetivo de realizar auditorias e investigação, caso necessário.

4.5 Cabe à CTIN a definição de critérios e requisitos de segurança para instalação, homologação e execução de programas de distribuição livre nas estações de trabalho da rede institucional.

4.5.1 Identificado programa instalado ou executando em desacordo aos critérios de segurança definidos, será registrado o incidente de segurança e comunicado à Coordenação responsável pelo patrimônio.

4.5.2 Caso haja necessidade em utilizar programa de computador não homologado ou licenciado pela CTIN, deve ser encaminhada solicitação de

instalação ou aquisição, acompanhada de justificativa para uso ou compra de produto ou serviço.

4.6 É vedada a instalação de programa licenciado para o IGEPPS em computador de mesa ou dispositivo portátil que não seja de propriedade desta Autarquia.

5. DAS ESTAÇÕES DE TRABALHO

5.1 A identificação das estações de trabalho do IGEPPS é realizada pela CTIN e deve estar de acordo com padrões por ela definidos.

5.2 As estações de trabalho são patrimônio de responsabilidade da sessão onde foram instalados, sendo vedada a transferência destes entre setores sem solicitação expressa a CTIN e ao GSA.

5.3 É vedado ao usuário o privilégio de administração e acesso à senha de administrador local da estação de trabalho.

5.4 É vedado ao usuário modificar a configuração da estação de trabalho, desabilitando ou desinstalação recursos de máquina ou segurança aplicados.

5.5 É vedado a abertura física ou desmontagem de equipamento de informática de propriedade do IGEPPS, exceto se realizados pela CTIN ou por pessoa ou empresa autorizada por este.

5.5.1 Esta ação só pode ser executada nas instalações da CTIN e acompanhadas pelo responsável técnico.

5.5.2 Uma vez recolhido equipamento para a manutenção técnica, a responsabilidade deste patrimônio é da CTIN sendo necessário adotar medidas que salvaguardem a integridade deste equipamento.

5.5.3 A CTIN fica isenta de responsabilidade sobre toda e qualquer informação armazenada localmente em equipamento de informática entregue.

5.6 É vedado a conexão à rede institucional do IGEPPS, por meio de cabeamento físico, de computador de mesa ou dispositivo móvel que não seja fornecido pelo IGEPPS.

5.6.1 No caso de necessidade de conexão à rede institucional de computador de fornecedor que utilize as dependências do IGEPPS, cabe à CTIN autorizar e definir os critérios e requisitos de segurança necessários.

5.7 Não é permitido gravar nas estações de trabalho e na rede do IGEPPS arquivos de áudio, filmes, fotos e *software* com direitos aurorais ou qualquer outro tipo que possa ser considerado pirataria.

5.8 Em caso de dano, inutilização ou extravio do equipamento o servidor deverá comunicar imediatamente à CTIN que deverá adotar as providências cabíveis.

5.9 Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo na CTIN, que deverá adotar as providências cabíveis.

5.10 Não é permitido retirar ou transportar qualquer equipamento de informática do setor de destino alocado sem autorização prévia da CTIN.

5.11 Fica proibida a utilização, sem devido consentimento, de equipamentos de informática por pessoas sem vínculo com o IGEPPS.

5.12 É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática.

5.12.1 Caso o equipamento esteja sem identificação de patrimônio, o setor GSA deverá ser notificado para que sejam adotadas as providências cabíveis.

5.13 A solução institucional de proteção *Endpoint* deve estar atualizada nas estações de trabalho e com a autoproteção ativa.

5.14 É de inteira responsabilidade do servidor ao receber o Termo de Responsabilidade sobre Recursos Computacionais, verificar as informações nele contidas como identificação patrimonial, nº de série, além dos seus dados pessoais, matrícula e Gerência/Coordenação vinculada ao Patrimônio.

5.15 É vedada a utilização de qualquer tipo de dispositivo de comunicação de rede como roteadores, switches, modens, repetidores e outro meio de comunicação de rede nas estações de trabalho do IGEPPS que não sejam fornecidas pela CTIN ou tenha a sua devida autorização.

6 DOS SERVIÇOS DE IMPRESSÃO

6.1. O serviço de impressão destina-se exclusivamente a atividades de cunho institucional.

6.2. A impressão de documentos deve ser evitada sempre que possível.

6.3. Recomenda-se usar impressão em face dupla e modo econômico sempre que possível.

6.4. Deve-se buscar a tramitação de processos sempre de forma eletrônica, fazendo o uso da impressão apenas nos casos em que se requer assinatura ou carimbo impresso.

6.5. As impressoras são alocadas nas Diretorias e Coordenadorias conforme demandas apresentadas.

6.6. Toda impressão realizada através do serviço deve ser associada a um único usuário.

6.6.1. Informações sobre número de páginas e títulos de documentos, data e hora de impressão e usuário responsável são registradas em sistema gestor do serviço e fornecedor do serviço.

6.7. O IGEPPS se reserva o direito de implementar política de quotas de impressão, a qualquer momento.

6.8. O fornecimento de insumos e manutenção nos equipamentos é de responsabilidade do fornecedor do serviço, cabendo à CTIN apenas a função de configuração de acesso à impressora da sessão na estação de trabalho e identificação de falha para o devido acionamento do suporte contratado.

6.9. Poderão ser implementados mecanismos para redução de custos tais como:

6.9.1. Limite de páginas por documento;

6.9.2. Redirecionamento de documentos grandes para impressoras de maior porte;

6.9.3. Limite de cópia por documento;

6.9.4. Tempo mínimo entre impressões;

6.9.5. Obrigatoriedade de autorização presencial para início de impressão.

6.10. As mesmas orientações se aplicam aos serviços de fotocópia e digitalização de documentos.

6.11. A CTIN é responsável pela infraestrutura mantenedora do serviço de impressão contratado - pontos lógicos de rede e servidor de impressão.

6.12. E vedada a utilização de qualquer porta ou meio de comunicação alternativo encontrado na impressora como NFC, USB, Bluetooth ou cabeamento de rede, que não seja a comunicação preestabelecida pela CTIN.

7 DOS DISPOSITIVOS PORTÁTEIS E DE REDE SEM FIO

7.1. A conexão de dispositivo portátil à rede institucional deve seguir procedimento específico definido pela CTIN:

7.1.1. Dispositivo portátil particular deve ser autorizado pela Coordenação imediata e com acesso apenas à Internet por meio da rede sem fio.

7.1.1.1. Uma vez autorizado, a configuração deste dispositivo à rede sem fio do IGEPPS é de responsabilidade da CTIN, sendo vetado em qualquer circunstância o fornecimento de chave de acesso ao ambiente.

7.1.1.2. As redes sem fios devem estar habilitadas com criptografias WPA2 ou protocolos de criptografias que estejam atualizados e considerados pelo CTIN como mais seguros, garantindo que, durante o trânsito das informações entre os dispositivos, a conexão esteja segura.

7.1.1.3. A utilização da rede sem fio interna deverá ser apenas utilizada para conexão de ativos de propriedade do IGEPPS e durante os trabalhos dos servidores. O sistema de acesso à rede sem fio deverá ser do tipo WPA2 *Enterprise ou superior*, que permite autenticação por usuários.

7.1.1.4. A CTIN também se revoga da obrigação em resolver problemas na utilização da rede sem fio do IGEPPS por dispositivos portáteis particulares.

7.1.2. Dispositivo portátil de propriedade do IGEPPS deve ser inserido no domínio do IGEPPS para a utilização dos recursos de rede associados às credenciais de acesso do servidor.

7.1.2.1. A CTIN revoga a responsabilidade em resolver problemas de acesso de dispositivos portáteis de propriedade do IGEPPS à rede de terceiros.

7.1.3. Ao utilizar rede de computadores externa por meio de dispositivos portáteis de propriedade do IGEPPS, o usuário deve obedecer também às normas e as diretrizes daquelas redes.

7.1.3.1. Em caso de divergência entre as normas de segurança da rede externa e o IGEPPS, prevalece a definição da PSI do IGEPPS.

7.2. Está vedada a utilização de rede sem fio em estações de trabalho local do IGEPPS, exceto quando solicitada a habilitação de interface de rede wireless ao CTIN através de documento autorizado pela Coordenação imediata.

Acesso Remoto – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1 Estabelecer critérios para a concessão e controle de acesso remoto feito pelos servidores autárquicos (efetivos e temporários) ao ambiente institucional do IGEPPS, para o desenvolvimento de suas atividades laborais em período extraordinário.

2. DEFINIÇÃO

2.1 Entende-se por ACESSO REMOTO: ingresso, por meio de uma rede pública, aos dados de computador fisicamente da máquina do usuário.

2.2 Rede Pública: rede de acesso a todos.

2.3 Termo de Responsabilidade: termo assinado pelo servidor concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

2.4 VPN: Rede Virtual Privada é uma rede de dados privada que faz uso de infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois recursos computacionais através de uma rede compartilhada ou pública de tal maneira que emula uma conexão ponto a ponto privada (rede local).

3. PARA ACESSO REMOTO

3.1. O acesso remoto aos serviços institucionais somente será disponibilizado aos servidores do IGEPPS que, oficialmente, executem atividades vinculadas à atuação desta Autarquia.

3.1.1. O acesso deve ser solicitado pela Coordenadoria vinculada ao servidor, justificando a necessidade deste acesso e definindo a periodicidade.

3.1.2. A tramitação desta solicitação dar-se-á através do Sistemas de Chamados da CTIN e deverá ser autorizada pelo Gabinete da Presidência.

3.2. A liberação do acesso remoto só será efetivada após as autorizações gerenciais envolvidas apresentarem pelo sistema de chamados GLPI a sua manifestação, ficando sob responsabilidade da CTIN notificar ao servidor, sua liberação de acesso.

3.2.1. Será enviado para o e-mail do solicitante o manual de orientação para a configuração do acesso remoto privado e a customização de seu acesso à rede do IGEPPS.

3.2.2. A configuração de dispositivo portátil ou computador de mesa pessoal é de responsabilidade do servidor autorizado, ficando a CTIN isento de responsabilidade sobre a integridade dos sistemas instalados neste equipamento.

3.3. As conexões remotas à rede institucionais do IGEPPS devem ocorrer da seguinte maneira:

3.3.1. Utilização de autenticação forte;

3.3.2. As senhas e informações que trafegam entre a estação remota e a rede do IGEPPS devem ser criptografadas;

3.3.3. É vedada a utilização do acesso remoto para fins não relacionados às atividades do Instituto.

3.3.4. É vedada a utilização deste recurso com colaboradores sem vínculo institucional.

3.3.4.1. A exceção é aplicada aos fornecedores de Tecnologia da Informação mediante assinatura de Termo de Confidencialidade e cláusula explícita em Contrato de Prestação de Serviços.

3.4. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

3.4.1. Finalização do período solicitado ou término do Contrato;

3.4.2. Perda de necessidade de utilização do serviço;

3.4.3. Transferência do usuário para outra secretaria ou autarquia do Governo do Estado do Pará;

3.4.4. Identificação de vulnerabilidade, risco ou uso indevido.

3.4.5. Por ordem expressa do Presidente desta Autarquia.

3.5 A CTIN poderá supervisionar e auditar as pessoas/servidores que possuem autorização de acesso à VPN. Em caso de identificação de permissão irregular, a CTIN deverá imediatamente revogar o acesso do servidor/fornecedor e, se necessário, reportar ao seu superior.

Monitoramento e Controle de Acesso Físico – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1. Estabelecer critérios para a concessão de acesso as dependências físicas desta Autarquia e seus limites técnico-operacionais assim como controle de acesso ao sistema de filmagem em atividade do IGEPPS.

2. DEPENDÊNCIAS FÍSICAS DO IGEPPS

2.1. O acesso ao prédio central do IGEPPS dar-se-á através da Guarita Principal seguindo orientação do vigilante/segurança.

2.2. O controle de acesso físico às dependências desta Autarquia, é feito primeiramente na recepção do térreo, através de seu cadastramento, e posterior acesso as dependências do IGEPPS mediante autorização de acesso por parte do servidor público contactado nesta visita.

2.3. Para o controle do acesso interno de seus servidores e fornecedores residentes, esta Autarquia deve realizar o cadastramento prévio destes em sistema informatizado de reconhecimento biométrico-facial e disponibilizar os recursos computacionais necessários para autenticação e reconhecimento de acesso destes.

2.3.1. É de responsabilidade da CTIN a manutenção da infraestrutura lógica e de dados do ambiente.

2.3.2. A Gestão do Sistema de Acesso Funcional do IGEPPS é de responsabilidade da Coordenadoria de Desenvolvimento de Pessoas (CODP).

2.4. Cabe às coordenadorias desta Autarquia a solicitação à CODP de cadastramento de novos servidores e fornecedores.

3. DATACENTER E SALAS TÉCNICAS

3.1. Os controles de acesso físico visam restringir o acesso aos equipamentos de tecnologia da informação.

3.2. O acesso ao Datacenter e as Salas Técnicas somente poderá ser feito por pessoas autorizadas da CTIN.

3.3. O acesso de visitantes ou terceiros ao Datacenter e Salas Técnicas somente poderá ser realizado com acompanhamento de um servidor da área de Tecnologia da Informação da CTIN.

3.4. As dependências físicas do Datacenter e Sala Técnica devem ser mantidas limpas e organizadas. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do COAS/GSA.

3.5. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

3.6. A temperatura ambiente destes locais não pode ultrapassar os 32ºC (trinta e dois graus Celsius). Sendo adequada uma temperatura entre 15 graus Celsius e 32 graus Celsius, bem como uma umidade relativa de 20% a 80%.

4. MONITORAMENTO – CÂMERAS DE FILMAGEM

4.1. O IGEPPS fará uso de câmeras de segurança instaladas em suas dependências, ficando resguardada a dignidade humana de seus servidores e colaboradores, sendo vedada a instalação de câmeras e escutas em banheiros e lavabos.

4.1.1. As câmeras de segurança estão prioritariamente instaladas em áreas de circulação comum dentro da estrutura predial do IGEPPS, salas técnicas e datacenter, acesso a saída de emergência, acesso ao refeitório, garagem, guaritas de acesso e imediações públicas.

4.1.2 É vedada a instalação de câmeras ou escutas em locais que não estejam sobre a visibilidade de todos.

4.2. A filmagem descrita nesta normativa tem por objetivo verificar o respeito dos usuários às regras estabelecidas no presente documento, bem como assegurar

segurança física aos titulares, não constituindo qualquer violação a intimidade, vida privada, honra ou imagem da pessoa filmada.

4.3. As imagens captadas dentro das dependências do IGEPPS serão arquivadas pelo período necessário para atingimento da finalidade de monitoramento pretendida e mantidas em caráter estritamente confidencial, somente podendo ser acessadas pelos servidores autorizados em caso de infração as regras constantes na PSI e suas normativas e/ou infração de legislação vigente.

4.3.1. O sistema atual de vigilância eletrônica foi doado ao IGEPPS pelo empreiteiro responsável pela construção das dependências atuais da Entidade. Dito isso, registramos que o modelo de equipamentos sobrescreve os arquivos de imagem mais antigos em face ao volume de dados salvos diariamente e principalmente limitado ao espaço interno disponível no equipamento.

4.3.2. Trata-se de sistema que não dispõe de recursos que permitam a captura e salvaguarda de informações em recurso compartilhado de rede.

4.4. A monitoração ativa das áreas externo-predial do IGEPPS é feita por equipe de segurança patrimonial contratada, sendo vedado a estes, acesso as demais dependências.

4.4.1. É de responsabilidade da CTIN a garantia da infraestrutura lógica do ambiente e disponibilização ao sistema de monitoramento proprietário instalado em máquinas fora do domínio institucional.

Acesso à Internet – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1. Estabelecer critérios para a administração e utilização de acesso aos serviços de Internet no âmbito do IGEPPS.

2. DIRETRIZES GERAIS

2.1. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela Autarquia.

2.2. Cada usuário é responsável pelas ações e acessos realizados por meio de seu perfil de Acesso.

2.3. O perfil de acesso à internet se aplica ao grupo de servidores lotados em determinada sessão desta Autarquia ou grupo de funcionários que precisam coletivamente ter acesso a determinado serviço excludente.

2.4. Os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade do Instituto, que pode analisar e, se necessário, bloquear qualquer arquivo, site, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta normativa.

2.5. Toda alteração de perfil de acesso somente será realizada mediante solicitação formal, pela Coordenadoria vinculada ao servidor, contendo a devida justificativa, que será avaliada pela CTIN, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade à segurança e à integridade da rede do IGEPPS.

2.5.1. A autorização desta solicitação será aplicada ao perfil de acesso, comum a todos os servidores lotados na Coordenação e/ou Diretoria solicitante.

2.5.2. Toda solicitação de acesso ou mudança de perfil deve ser registrado no sistema de chamados da CTIN.

2.6. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

2.6. 1. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

2.6.2. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do IGEPPS;

2.6.3. Uso recreativo da internet em horário de expediente;

2.6.4. Uso de *proxy* anônimo, VPN distinta da rede que não seja do próprio IGEPPS, ou qualquer outro subterfúgio que permita a navegação anônima ou fora da rede preestabelecida pelo IGEPPS;

2.6.5. Acesso à rádio e TV em tempo real;

2.6.6. Acesso a jogos e similares;

2.6.7. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

2.6.8. Envio a destino externo de qualquer *software* licenciado ou documento de propriedade do IGEPPS;

2.6.9. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do IGEPPS;

2.6.10. Utilização de *software* de compartilhamento de conteúdo na modalidade *peer-to-peer* (P2P);

2.6.11. Uso de serviços de compartilhamento e armazenamento em nuvem, pública ou privada, de informações sob a responsabilidade desta Autarquia.

2.6.12. Uso de redes sociais e serviços de comunicação por mensagens;

2.6.13. Uso de e-mail particular.

2.7. Caso a Autarquia julgue necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho, a produtividade ou a segurança das atividades do servidor, bem como, que exponham a rede a riscos de segurança.

2.8. É proibido utilizar os recursos do IGEPPS para fazer o *download* ou distribuição de *software* ou dados não legalizados.

2.9. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet imediatamente bloqueado, sendo comunicado o fato à chefia imediata.

2.9.1. Registrada e comprovada a infração a esta normativa, o servidor está passível de responder processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

2.10. A CTIN, com apoio da Diretoria Executiva do IGEPPS, utiliza solução de segurança específica para controle de acesso por filtro de conteúdo *web*, filtro de aplicação, inspeção em profundidade e registro e recuperação de *log* de acesso em tempo real, visando a interceptação para verificação de acessos não autorizados, conforme critérios de segurança definidos.

2.11. O monitoramento dos sites é ativo e diário, visando minimizar a ocorrência de ameaças e comprometimento de performance da rede lógica e/ou acessos indevidos à internet.

Serviços de Mensageria – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1. Estabelecer critérios para disponibilização dos serviços de correio eletrônico institucional do IGEPPS aos servidores autárquicos - ativos, temporários e comissionados - e o *chat* institucional que atenderá a todo usuário com permissão de acesso à rede do IGEPPS.

2. E-MAIL INSTITUCIONAL

2.1. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do IGEPPS.

2.2. São usuários do serviço de correio eletrônico institucional, os servidores autárquicos que executem atividade vinculada à atuação do IGEPPS.

2.2.1. Entende-se por servidor autárquico os funcionários efetivos, temporários comissionados vinculados a esta Autarquia.

2.3. A concessão de contas de correio eletrônico será mediante solicitação da Coordenadoria vinculado ao servidor público.

2.4. Poderá ser solicitada a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação.

2.5. É vedado o acesso ao conteúdo das mensagens transitadas por meio do serviço de correio eletrônico institucional, salvo nas hipóteses previstas em lei.

2.5.1. Caso seja necessária tal ação, deve-se abrir chamado a CTIN junto com o fornecedor do serviço de correio corporativo para o resgate destas informações e ser entregue para a autoridade policial.

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

2.7. É vedado ao usuário o uso do serviço de correio eletrônico e da ferramenta de chat institucionais com o objetivo de:

2.7.1. Praticar crimes e infrações de qualquer natureza;

2.7.2. Executar ações nocivas contra outros recursos computacionais do IGEPPS ou de redes externas;

2.7.3. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e ao Código de Ética do IGEPPS;

2.7.4. 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 IGEPPS;

2.7.5. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pelo IGEPPS;

2.7.6. Divulgar, no todo ou em parte, os endereços eletrônicos institucionais constantes do catálogo de endereços do serviço de e-mail do IGEPPS;

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

2.7.8 Praticar qualquer espécie de exploração sexual;

2.7.9 Praticar qualquer tipo de pornografia;

2.7.10 Praticar qualquer forma de ameaça, chantagem e assédio moral ou sexual;

2.7.11 Praticar qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

2.7.12 Praticar preconceito baseado em cor, sexo, orientação sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

2.7.13 Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;

2.7.14 Praticar e/ou a incitar crimes ou contravenções penais;

2.7.15 Praticar propaganda política nacional ou internacional;

2.7.16 Desrespeitar à imagem ou aos direitos de propriedade intelectual e industrial do IGEPPS;

2.7.17 Tentar expor a infraestrutura computacional do IGEPPS.

2.8. É de responsabilidade do usuário do correio eletrônico:

2.8.1. Manter em sigilo sua senha de acesso ao correio institucional;

2.8.2. Desconectar do portal de acesso toda vez que se ausentar, evitando o acesso indevido;

2.8.3. Comunicar imediatamente a CTIN, preferencialmente através do Sistema de Chamados GLPI ou pelo endereço **ctin@igeprev.pa.gov.br**, do recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;

2.8.4. Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo;

2.9. É de responsabilidade da Coordenadoria de Tecnologia da Informação (CTIN):

2.9.1. Criar e manter cadastro das caixas de e-mail institucional dos servidores do IGEPPS das listas de distribuição;

2.9.2. Cancelar os acessos ao serviço de correio eletrônico dos servidores que se desvinculem desta Autarquia;

2.9.3. Propor a divulgação de orientação sobre o uso correto do correio eletrônico;

2.9.4. Desenvolver demais ações que garantam a operacionalização desta normativa.

2.10. Cabe às Coordenações e Gerências desta Autarquia comunicar o desligamento do servidor, para que o e-mail seja encerrado.

2.11. É de responsabilidade da CTIN a criação e administração básica das caixas de correio eletrônico institucional e listas de distribuição do IGEPPS.

2.12. Qualquer ação além das atribuições citadas no item anterior será demandada ao fornecedor do serviço.

3. CHAT INSTITUCIONAL

3.1. É de uso obrigatório, para a comunicação interna entre equipe ou setores, o uso da solução de mensagens instantâneas "MICROSOFT *TEAMS*" disponível na área de trabalho das máquinas associadas ao domínio institucional.

3.2. Por padrão, o acesso será prioritariamente entre servidores de cada Coordenadoria ou Gerência.

3.2.1. Caso seja necessário contato com servidor de sessão diferente a sua, basta o usuário adicionar o contato através de seu nome completo.

3.3. As orientações para acesso à ferramenta serão repassadas pela CTIN através de Manual de Orientação disponível no site da intranet.

3.4. Será vedada a utilização do CHAT institucional para produzir, transmitir ou divulgar mensagem que:

3.4. 1. Contenha qualquer ato ou forneça orientação que concite ou contrarie os interesses do IGEPPS;

3.4.2. Contenha conteúdo considerado impróprio, obsceno, ilegal ou de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico ou que contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

3.4.3. Contenha fins políticos locais ou do país (propaganda política);

3.4.4. Vise a obtenção de acesso não autorizado a outro equipamento, servidor ou rede, ou ainda, que burle qualquer sistema de segurança;

3.4.5. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

3.4.6. Vise acessar informações restritas ou sigilosas sem explícita autorização do proprietário da informação;

3.4.7. Contenha ameaças eletrônicas (*malwares*) nocivas aos recursos computacionais do IGEPPS.

Backup – IGEPPS

Versão 02 – 12/2024

1. OBJETIVO

1.1. Estabelecer critérios para execução de serviço de realização de cópia de segurança de arquivos, sistemas e serviços – ativos e legados – e sua recuperação íntegra e contável, quando necessária.

2. ORIENTAÇÃO

2. 1. Todos os *backups* devem ser automatizados por sistemas especialistas para que sejam executados preferencialmente em horários que não interfiram na atividade fim desta Autarquia.

2.2. Sobre os *Jobs*/Tarefas de *backup*:

2.2.1. Para servidores críticos devem ser realizadas diariamente, atendendo janela de manutenção disponível, com um mês de retenção;

2.2.2. Para máquinas físicas devem ser realizadas diariamente, atendendo janela de manutenção disponível, com um mês de retenção;

2.2.3. Para máquinas virtuais (VM) devem ser realizadas diariamente, atendendo janela de manutenção disponível, com um mês de retenção;

2.2.4. Para serviços e servidores do ambiente legado deve ser realizado mensalmente, atendendo janela de manutenção disponível, com retenção das últimas 3 cópias.

2.3. Restauração de arquivos terá um prazo máximo de 30 dias para a sua recuperação, não sendo possível recuperar arquivos mais antigos que esse período.

2.4. A sincronização das cópias de *backup*, entre os sites dos IGEPPS, deve ser realizada diariamente em janela que não afere o desempenho de rede.

2.5. Cabe à CTIN, suportado pelo fornecedor de solução proprietária, prever e executar testes periódicos de restauração, no intuito de averiguar a integridade e

legitimidade dos dados salvaguardados e principalmente validar os processos empregados e estabelecer plano de melhoria contínua.

2.6. Cabe à CTIN, suportado pelo fornecedor de solução proprietária, identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o *software* não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

2.7. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro e distantes o máximo possível do Datacenter.

2.7.1. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

2.8. Solicitações de restauração de arquivos, serviços ou máquinas devem ser registradas no sistema de abertura de chamados, devendo conter informações pertinentes à identificação do objeto a ser restaurado e datado para definir o ponto de recuperação.

2.9. Cabe à CTIN manter a disponibilidade física e lógica da solução de *backup* em produção no IGEPPS.

2.10. Cabe à CTIN o armazenamento em local seguro, bem como criptografia dos dados armazenados.

2.11. Cabe à CTIN a destruição das mídias que deverão ser inutilizadas (item 2.7.1), cabendo a ela tomar medidas para inviabilizar acesso aos dados, como a destruição efetiva de mídia.

CONTROLE DE VERSÃO			
SETOR TÉCNICO RESPONSÁVEL			CTIN / SEGURANÇA
Versão	**Data**	**Autor**	**Alteração**
1.0	09/11/20	Juliana Amaral	Documento inicial para estabelecimento de marco inicial da PSI
2.0	06/12/24	Keytson Portugal	Alteração documental de melhorias e inserções de novas políticas de segurança da informação.