PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas Administrativas

Versão 0.0

Aprovada em 27/08/2020

Portaria Normativa nº22/2020 - PR

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas Administrativas

Sumário

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do IPASGO para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores, associados, clientes e prestadores de serviços do IPASGO seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa, das informações e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do IPASGO quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, com as devidas autorizações.

3. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados, auditadas e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Planejamento e Sistemas de Informações sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo IPASGO pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes, caso seja aplicável.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços, porém, fica a cargo do IPASGO realizar eventuais monitoramento, auditoria e inspeções sem prévio aviso.

O IPASGO, por meio da Gerência de Planejamento e Sistemas de Informações, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5. REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores, clientes, prestadores de serviços a fim de que a política seja cumprida dentro e fora da empresa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos do IPASGO a Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores e prestadores de serviços. Todos os colaboradores e prestadores de serviços devem ser orientados sobre os procedimentos de segurança, bem

como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Planejamento e Sistemas de Informações e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo IPASGO ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

O IPASGO exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, associados, clientes e prestadores de serviços reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI foi implementada no IPASGO por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

6. DAS RESPONSABILIDADES ESPECIFICAS

6.1. Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao IPASGO e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2. Dos Colaboradores em Regime de Exceção (temporários, estagiários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

6.3. Dos Prestadores de Serviços

Deve se constar em contrato com todos os prestadores de serviços clausulas de sigilo, confidencialidade e de responsabilidade a fim de atribuir e responsabilizar aqueles que fizerem o mal uso das informações e/ou cometerem atos ilícitos ou má conduta profissional.

6.4. Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores e prestadores de serviços sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do IPASGO.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPASGO.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como outras políticas relacionadas.

6.5. Dos Custodiantes da Informação

6.5.1. Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e pelas Normas de Segurança da Informação complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e técnicas a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente utilizado pelos associados e prestadores de serviços, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o IPASGO. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente do associado, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados

digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos do IPASGO;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos IPASGO;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

6.5.2. Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do IPASGO.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do IPASGO, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o IPASGO.

Buscar alinhamento com as diretrizes corporativas da instituição.

6.5.3. Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

A composição mínima deve incluir um colaborador de cada uma das áreas: Tecnologia, Jurídico, Compliance, Financeiro e Gestão de Pessoas;

Deverá o CSI reunir-se ordinariamente uma vez ao mês. Reuniões extraordinárias devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o IPASGO ou mediante a convocação do seu Presidente.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

• propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

• propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;

• avaliar os incidentes de segurança e propor ações corretivas;

• definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

6.6. Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, bem como seu devido cumprimento o IPASGO poderá:

• 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 poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

7. CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores do IPASGO quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do IPASGO é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o IPASGO e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do IPASGO:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- 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;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPASGO ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das áreas do IPASGO estiver sujeita a algum tipo de investigação;

- produzir, transmitir ou divulgar mensagem que:

  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPASGO;
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha 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;
  - vise obter acesso não autorizado a outro computador, servidor ou rede;
  - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - vise burlar qualquer sistema de segurança;
  - vise vigiar secretamente ou assediar outro usuário;
  - vise acessar informações confidenciais sem explícita autorização do proprietário;
  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - inclua imagens criptografadas ou de qualquer forma mascaradas;
  - contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 20 MB para recebimento (internet)
  - tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  - tenha fins políticos locais ou do país (propaganda política);
  - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
  - As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
    - Nome do colaborador
    - Gerência ou departamento
    - Nome da empresa
    - Endereço da Unidade Administrativa
    - Telefone(s)
    - Correio eletrônico
    - Endereço do site institucional

8. INTERNET

Todas as regras atuais do IPASGO visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o IPASGO, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O IPASGO, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades e que não prejudique a imagem do IPASGO.

Como é do interesse do IPASGO que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome do IPASGO para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

8.1. UTILIZAÇÃO

O uso da Internet e dos recursos de tecnologia pelos colaboradores do IPASGO é permitido, sugerido e incentivado, desde que seu uso esteja relacionado aos objetivos e atividades fins do negócio ou responsabilidades do colaborador.

Entretanto, o IPASGO tem como exigência para o uso da Internet e dispositivos móveis que os colaboradores:

- Sigam a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias);
- Usem a Internet de forma responsável, consciente e munidos de bom senso;
- Utilizem smartphones para atividades pessoais somente quando necessário;
- Não criem riscos desnecessários para os equipamentos, informações ou para o negócio do IPASGO.

No caso de dúvidas ou sugestões sobre a política de uso da Internet e recursos de tecnologia, o colaborador deve entrar em contato com seu gestor ou responsável direto.

Fica estabelecido que os colaboradores do IPASGO são os membros, servidores e os demais agentes públicos ou participantes que oficialmente executem atividades vinculadas à atuação do IPASGO.

8.2. REGRAS DE ACESSO E UTILIZAÇÃO DE RECURSOS

A. REGRAS GERAIS

- O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo IPASGO, observando-se sempre a conduta compatível com a moralidade administrativa. Para este acesso os colaboradores utilizarão seus usuários de rede, usado para efetuar logon nas estações de trabalho corporativas do IPASGO;

- Toda e qualquer conta de usuário possuirá níveis de acesso distintos (**veja detalhes no ANEXO I**), obedecendo as necessidades legais das atribuições dos cargos dos colaboradores. Estes níveis de acesso serão definidos pela **Gerência de Planejamento e Sistemas de Informação – GPSI**;

- Fica sob responsabilidade da GPSI, em comum acordo com os responsáveis legais pela aprovação e oficialização deste documento, tratativas relacionadas à quaisquer exceções à regra citada acima;

- Exceções que proporcionem riscos de segurança da informação para o IPASGO deverão ser negadas e justificadas pela GPSI;

- Toda alteração de nível de acesso já existentes somente será realizada mediante solicitação formal, pelo gerente imediato do colaborador, contendo a devida justificativa, que será avaliada pela GPSI, podendo esta solicitação ser negada caso necessário, mediante justificativa;

- Cada colaborador é responsável pelo uso de suas credenciais de acesso. Considerando que a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em segredo, sendo o colaborador responsabilizado por qualquer transação efetuada durante o seu uso;

- Os colaboradores devem estar capacitados para utilização da Internet de forma consciente e segura. Para aqueles que não se sentirem capacitados, a orientação é que entrem em contato com a GPSI para maiores orientações;

- Os navegadores utilizados corporativamente, em estações de trabalho corporativas, deverão ser homologados pela GPSI sem quaisquer exceções;

- Solicitações de liberação de determinado site deverão ser formalizadas à GPSI através dos meios oficiais, informando:

    - Nome completo;
    - Departamento;
    - Ramal;
    - Justificativa detalhada.

- As solicitações citadas acima serão tratadas pela GPSI, cabendo à mesma a responsabilidade de aprovação ou não à solicitação.

PROIBIDO E INACEITÁVEL

- Uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente do IPASGO;

- Acesso às páginas de conteúdo considerado ofensivo, ilegal ou impróprio, que por motivos técnicos ainda não forem classificadas e bloqueadas por padrão. Entende-se por conteúdo ofensivo, ilegal ou impróprio:

    - Pornografia;
    - Pedofilia;
    - Violência;
    - Jogos e Apostas;
    - Chats de bate-papo não corporativos;
    - Rádios e Televisão em tempo real;
    - Quaisquer outros conteúdos notadamente fora do contexto do trabalho desenvolvido, como fóruns de discussão e blogs não profissionais.

- Acessar ou obter na Internet arquivos que apresentem vulnerabilidades de Segurança da Informação ou que possam comprometer, de alguma forma, a segurança e integridade da rede do IPASGO;

- Uso de mensageiro instantâneo não homologado ou autorizado pela GPSI;

- Utilização de quaisquer serviços de proxy anônimo;

- Divulgação de informações confidenciais do IPASGO por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, serviços de armazenamento na nuvem ou ferramentas semelhantes;

- Envio a destino externo de qualquer software licenciado ao IPASGO, dados de sua propriedade ou de seus colaboradores, exceto sob autorização legal e devidamente documentada pelo responsável de sua guarda;

- Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do IPASGO;

- Utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);

- Utilização de serviços de armazenamento em nuvem, não corporativa ou não autorizada pela GPSI;

- Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação do IPASGO, na forma definida pela GPSI;

- Utilização dos equipamentos de tecnologia para executar quaisquer tipos ou formas de fraude ou pirataria;
- Envio de material ofensivo ou de assédio para outras pessoas ou entidades;
- Baixar (download) qualquer tipo de software ou material cujo direito pertença a terceiros, sem ter um contrato de licenciamento ou outros tipos de licença;
- Realizar atividades de navegação ou download que comprometam o desempenho da Internet ou da rede corporativa;
- Pesquisar ou tentar obter informações em áreas ou setores que não possuem autorização (hacking);
- Criar ou transmitir qualquer tipo de material difamatório entre colaboradores do IPASGO ou na internet;
- Utilizar os recursos do IPASGO para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
- Realizar quaisquer atividades pessoais que não tenham relação com as tarefas de sua responsabilidade no IPASGO e que gerem perda de foco no trabalho;
- Utilizar dispositivos móveis pessoais de forma exagerada para atividades pessoais, como acesso a e-mail, redes sociais e sistemas de comunicação;
- Utilização de quaisquer tipos de tecnologia de streaming de vídeo ou áudio ou plataformas de compartilhamento de vídeos e áudios e mídias sociais que não tenham relação com as responsabilidades no IPASGO, que comprometam a produtividade em horário de expediente e/ou performance da rede;
    - Tecnologias citadas acima poderão ter seu acesso liberado, para fins recreativos, mediante cumprimento de regra abaixo.
- Uso recreativo da Internet em horário de expediente;
    - O uso recreativo poderá ser autorizado em horário de almoço, entre às 11:30 e 13:30, de forma controlada, visando o não comprometimento de performance da rede interna do IPASGO e da Internet, cumprindo todas as demais regras presentes neste documento;

- Fica estabelecido como definição de uso recreativo da Internet no IPASGO: “Quaisquer tecnologias classificadas como mídias sociais, streaming de áudio e vídeo e compartilhamento de áudio e vídeo”;
- Fica sob responsabilidade da GPSI e responsáveis legais pela aprovação e oficialização deste documento, a definição dos controles aplicados para acesso à estas tecnologias.

- Realizar compras pessoais na Internet e tão pouco definir o endereço do IPASGO para entrega de qualquer tipo de encomenda;

- Realizar download de softwares que tenham direitos autorais, marca registrada ou patente na internet;

- Fornecer à si mesmo ou a terceiros senhas e acessos remotos não autorizados pela GPSI a recursos corporativos ou qualquer tipo de dado restrito ao IPASGO.

8.3. REDE SEM FIO

O acesso especifico à rede sem fio (WI-FI) do IPASGO é de uso exclusivo de usuários com credenciais de acesso e/ou autorizados previamente pela Gerência de Planejamento e Sistemas de Informações.

O IPASGO disponibiliza uma rede sem fio de eventos durante a realização dos mesmos, para visitantes onde há o exclusivo acesso à Internet e com regras de controle de conteúdo. Este ambiente é segregado do ambiente corporativo, e seus usuários utilizam credenciais de acesso temporárias;

O IPASGO disponibiliza uma rede sem fio para dispositivos móveis apenas para usuários previamente autorizados. Este ambiente é segregado;

A utilização da rede sem fio é uma concessão do IPASGO aos usuários que necessitem deste recurso para desempenhar suas funções e poderá ser suspensa, a qualquer momento, sem aviso prévio, caso sejam identificadas situações que possam comprometer a rede de dados do IPASGO.

A liberação de acesso, só será efetivada após avaliação e aprovação pela Gerência de Planejamento e Sistemas de Informações, para que se evitem ameaças à integridade e sigilo das informações contidas na rede do IPASGO.

Será feita uma análise criteriosa, podendo ser negado o acesso caso comprometa a segurança da rede do Instituto.

A solicitação de acesso deve ser registrada por e-mail, para suporte@ipasgo.go.gov.br e conter, no mínimo, as seguintes informações:

- Tipo da solicitação;
- Tempo de validade do acesso;
- Justificativa;
- Dados do solicitante;
- Dados do usuário.
- Anexar o termo de responsabilidade de uso da rede sem fio devidamente assinado.
- A disponibilização de acesso à rede sem fio de eventos deve obedecer às seguintes regras:
- Deve ser solicitada por gerentes ou superiores;
- O acesso é temporário e limitado às necessidades de negócio;
- Sua solicitação deve ocorrer antecipadamente, com no mínimo 3 dias de antecedência.
- A responsabilidade de todos os acessos feitos durante sua disponibilização é atribuída ao solicitante.

8.4. MONITORAMENTO

O IPASGO reafirma que o uso da tecnologia e da Internet é uma ferramenta valiosa para o desempenho das atividades da empresa e para todo o negócio. Dessa forma, o mau uso desses recursos pode ter impacto negativo sobre a produtividade dos colaboradores e os resultados do negócio.

Portanto, o IPASGO se dá o direito de aplicar restrições de navegação e monitorar o uso da Internet na rede corporativa, de forma individual, aplicando a cada equipamento e colaborador.

Através do serviço da GPSI, são aplicadas regras de navegação definidas de acordo com este documento, com o objetivo de garantir maior foco e produtividade dos colaboradores, bem como assegurar um ambiente digital controlado e seguro. Da mesma forma é registrado todo e qualquer tipo de acesso Internet por cada equipamento conectado à rede.

Todas as ferramentas de monitoramento ao acesso à Internet são de responsabilidade e controle da GPSI, podendo à mesma fornecer aos demais departamentos do IPASGO relatórios de acesso pontuais, para acompanhamento, com periodicidade a ser definida.

8.5. SANÇÕES

Comprovada a utilização irregular, o colaborador envolvido terá o seu acesso à Internet bloqueado pela GPSI, sendo comunicado o fato à gestão imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, podendo o colaborador envolvido responder disciplinarmente e/ou civilmente por eventuais prejuízos que vier a ocasionar ao IPASGO, podendo resultar em seu desligamento e, se aplicáveis, eventuais processos criminais.

ACESSO REMOTO

O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividade vinculada à atuação institucional do IPASGO e que necessitam desde serviço para execução de suas atividades institucionais, desde que autorizados.

Os administradores da rede do IPASGO lotados na Gerência de Planejamento e Sistemas de Informações, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais do Instituto quando necessário.

Os Representantes de Informática, quando administradores de rede e sistemas das unidades da IPASGO, poderão ter permissão de acesso aos servidores de rede e estações de trabalho de sua circunscrição quando necessário.

A liberação de acesso remoto, só será efetivada após avaliação e aprovação pela GPSI, para que se evitem ameaças à integridade e sigilo das informações contidas na rede do IPASGO.

Todos os usuários são responsáveis pelas informações e pelos recursos de informática a que tenham acesso.

Os usuários devem relatar formalmente a ocorrência ou suspeita de incidentes de segurança.

Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança da rede do Instituto.

A solicitação de acesso remoto deve ser registrado por e-mail, csi@ipasgo.go.gov.br e conter, no mínimo, as seguintes informações:

a) Tipo da solicitação;
b) Tempo de validade do acesso remoto;
c) Justificativa;
d) Dados do solicitante;
e) Dados do usuário.
f) Anexar o termo de responsabilidade - Anexo I

A disponibilização de acesso remoto à rede da IPASGO para outras organizações deve obedecer às seguintes regras:

a) Acesso temporário e limitado às necessidades de negócio;
b) Revisão periódica dos direitos de acesso;
c) Utilização de solução que permita a implementação e controle de regras de acesso.
d) O serviço de acesso remoto deve ser cancelado sob as seguintes condições:
e) Finalização do período especificado na solicitação ou contrato;
f) Perda da necessidade de utilização do serviço;
g) Transferência do usuário para outras unidades;
h) Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

As conexões remotas à rede da IPASGO devem ocorrer da seguinte maneira:

a) Utilização de autenticação;
b) As senhas e as informações que trafegam entre a estação remota e a rede do IPASGO devem estar criptografadas;

Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

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

🗁🗀🖋 IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o IPASGO e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados no IPASGO, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o IPASGO e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Gerência de Gestão de Pessoas do IPASGO é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Gestão de Pessoas responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Planejamento e Sistemas de Informações do IPASGO.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade). Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 32 (trinta e dois) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Gerência de Gestão de Pessoas deverá imediatamente comunicar tal fato a Gerência de Planejamento e Sistemas de Informações, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se

encerrado, bem como aos usuários de testes e outras situações similares. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

🗁🗁🖋COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do IPASGO, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Planejamento e Sistemas de Informações do IPASGO, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Planejamento e Sistemas de Informações e/ou à Gerência de Apoio Logístico e Suprimentos, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio do IPASGO (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores do IPASGO e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Planejamento e Sistemas de Informações.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

a) Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Planejamento e Sistemas de Informações do IPASGO, que terá acesso a elas para manutenção dos equipamentos.
b) Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
c) É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Planejamento e Sistemas de Informações do IPASGO ou por terceiros devidamente contratados para o serviço.
d) Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.
e) É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
f) O colaborador deverá manter a configuração do equipamento disponibilizado pelo IPASGO, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
g) Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

h) Todos os recursos tecnológicos adquiridos pelo IPASGO devem ter imediatamente suas senhas padrões (default) alteradas.
i) Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do IPASGO.

j) Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
k) Burlar quaisquer sistemas de segurança.
l) Acessar informações confidenciais sem explícita autorização do proprietário.
m) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
n) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
o) Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
p) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
q) Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente

atualizada, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso, bem como assinar o Termo de Responsabilidade.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Setor de Serviços Gerais.

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

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

13. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas

chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para 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.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

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

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do IPASGO, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

14. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do IPASGO. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição. Sendo assim, deverá sempre estar atento ao Código de Ética e Conduta IPASGO.

ANEXO I

PERFIS DE ACESSO À INTERNET

PERFIL AVANÇADO	
Categoria Adulto	
Classificações Liberadas	**Classificações Bloqueadas**
	× Aborto; × Álcool; × Crenças Alternativas; × Namoro; × Jogos de Azar; × Lingerie e Maiô; × Maconha; × Nudez e Risque; × Outros Materiais para adultos; × Pornografia; × Sexo Educacional; × Jogos de Guerra; × Tabaco; × Armas e Vendas;
	× Organizações de Advocacia.
Categoria Consumo de Largura de Banda	
Classificações Liberadas	**Classificações Bloqueadas**
	× Compartilhamento de arquivos ponto-a-ponto; × Compartilhamento e armazenamento de arquivos; × Download de freeware e software; × Radio e TV; × Telefone IP; × Download e Streaming de mídias; × Peer-to-Peer;
	× File Sharing;
Categoria Interesse Geral - Negócios	
Classificações Liberadas	**Classificações Bloqueadas**
➢ Negócios empresariais; ✓ Organizações de Caridade; ✓ Finanças e Bancos; ✓ Organizações Gerais; ✓ Governamentais e Jurídicas; ✓ Tecnologia da Informação; ✓ Segurança da Informação; ✓ Reunião Online ✓ Mecanismos de Pesquisa; ✓ Sites Seguros; ✓ Aplicações baseadas em Web; ✓ Forças Armadas;	× Acesso Remoto; × Web Hosting;
✓ Web Analytics	
Categoria Interesse Geral - Pessoal	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Arte e Cultura ✓ Corretagem e Negociação ✓ Educação Infantil ✓ Servidores de Conteúdo ✓ Cartões Postais ✓ Conteúdo Dinâmico ✓ Educação ✓ Entretenimento	× Publicidade × Leilão × Estacionamento de Domínio × Games × Conteúdo sem sentido × Chat Externo - IRC
✓ Folclore	

✓ Religião Global ✓ Saúde e Bem Estar ✓ Mensagem Instantânea ✓ Pesquisa de Emprego ✓ Medicina ✓ Notícias e Mídias ✓ Revistas e Grupos de Notícias ✓ Privacidade Pessoal ✓ Veículos ✓ Sites Pessoais e Blogs ✓ Organizações Políticas ✓ Imobiliária ✓ Enciclopédias ✓ Restaurante e Jantar ✓ Shopping ✓ Rede Social ✓ Sociedade e Estilo de Vida ✓ Esportes ✓ Viagem ✓ Mail - Web	
Categoria Potencialmente Responsável	
Classificações Liberadas	**Classificações Bloqueadas**
	× Abuso de Criança × Discriminação × Abuso de Drogas × Violência Explícita × Grupo Extremista × Hacking × Ilegal ou Antiético × Plágio × Site de Proxy
Categoria Riscos de Segurança	
Classificações Liberadas	**Classificações Bloqueadas**
	× DNS Dinâmico; × Sites Maliciosos; × Domínios sem categorização; × Phishing; × Spam - URL´s; × Domínios recentemente registrados;
Sites sem Categorias e exceções	
Bloquear por padrão todos os sites sem categoria; Exceções deverão ser listadas e liberadas somente para esta categoria	

PERFIL INTERMEDIÁRIO	
Categoria Adulto	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Organizações de Advocacia	× Aborto; × Álcool; × Crenças Alternativas; × Namoro; × Jogos de Azar; × Lingerie e Maiô; × Maconha; × Nudez e Risque; × Outros Materiais para adultos; × Pornografia; × Sexo Educacional; × Jogos de Guerra; × Tabaco; × Armas e Vendas;
Categoria Consumo de Largura de Banda	
Classificações Liberadas	**Classificações Bloqueadas**
	× Compartilhamento de arquivos ponto-a-ponto; × Compartilhamento e armazenamento de arquivos; × Download de freeware e software; × Radio e TV; × Telefone IP; × Download e Streaming de mídias; × Peer-to-Peer; × File Sharing;
Categoria Interesse Geral - Negócios	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Negócios empresariais; ✓ Organizações de Caridade; ✓ Finanças e Bancos; ✓ Organizações Gerais; ✓ Governamentais e Jurídicas; ✓ Tecnologia da Informação; ✓ Segurança da Informação; ✓ Reunião Online ✓ Mecanismos de Pesquisa; ✓ Sites Seguros; ✓ Aplicações baseadas em Web; ✓ Forças Armadas.	× Acesso Remoto; × Web Analytics; × Web Hosting;
Categoria Interesse Geral - Pessoal	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Arte e Cultura ✓ Educação Infantil ✓ Servidores de Conteúdo ✓ Saúde e Bem Estar ✓ Medicina ✓ Notícias e Mídias ✓ Organizações Políticas ✓ Enciclopédias ✓ Restaurante e Jantar ✓ Sociedade e Estilo de Vida	× Publicidade × Leilão × Estacionamento de Domínio × Games × Conteúdo sem sentido × Chat Externo – IRC × Corretagem e Negociação × Conteúdo Dinâmico × Entretenimento × Folclore × Mensagem Instantânea × Pesquisa de Emprego × Sites Pessoais e Blogs × Imobiliária × Revistas e Grupos de Notícias

	× Shopping × Mail – Web × Viagem × Cartões Postais × Educação × Religião Global × Rede Social × Privacidade Pessoal × Veículos × Esportes
Categoria Potencialmente Responsável	
Classificações Liberadas	**Classificações Bloqueadas**
	× Abuso de Criança × Discriminação × Abuso de Drogas × Violência Explícita × Grupo Extremista × Hacking × Ilegal ou Antiético × Plágio × Site de Proxy
Categoria Riscos de Segurança	
Classificações Liberadas	**Classificações Bloqueadas**
	× DNS Dinâmico; × Sites Maliciosos; × Domínios sem categorização; × Phishing; × Spam - URL´s; × Domínios recentemente registrados;
Sites sem Categorias e exceções	
Bloquear por padrão todos os sites sem categoria; Exceções deverão ser listadas e liberadas somente para esta categoria	

PERFIL BÁSICO	
Categoria Adulto	
Classificações Liberadas	**Classificações Bloqueadas**
	× Aborto; × Álcool; × Crenças Alternativas; × Namoro; × Jogos de Azar; × Lingerie e Maiô; × Maconha; × Nudez e Risque; × Outros Materiais para adultos; × Pornografia; × Sexo Educacional; × Jogos de Guerra; × Tabaco; × Armas e Vendas; × Organizações de Advocacia.
Categoria Consumo de Largura de Banda	
Classificações Liberadas	**Classificações Bloqueadas**
	× Compartilhamento de arquivos ponto-a-ponto; × Compartilhamento e armazenamento de arquivos; × Download de freeware e software; × Radio e TV; × Telefone IP; × Download e Streaming de mídias; × Peer-to-Peer; × File Sharing;
Categoria Interesse Geral - Negócios	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Organizações de Caridade; ✓ Governamentais e Jurídicas;	× Acesso Remoto; × Web Analytics; × Web Hosting; × Tecnologia da Informação; × Segurança da Informação; × Reunião Online × Mecanismos de Pesquisa; × Sites Seguros; × Aplicações baseadas em Web; × Forças Armadas. × Finanças e Bancos; × Organizações Gerais; × Negócios empresariais;
Categoria Interesse Geral - Pessoal	
Classificações Liberadas	**Classificações Bloqueadas**
✓ Arte e Cultura ✓ Saúde e Bem Estar ✓ Medicina	× Publicidade × Leilão × Estacionamento de Domínio × Games × Conteúdo sem sentido × Chat Externo – IRC × Corretagem e Negociação × Conteúdo Dinâmico × Entretenimento × Folclore × Mensagem Instantânea × Pesquisa de Emprego × Sites Pessoais e Blogs

	× Imobiliária × Revistas e Grupos de Notícias × Shopping × Mail – Web × Viagem × Cartões Postais × Educação × Religião Global × Rede Social × Privacidade Pessoal × Veículos × Esportes × Educação Infantil × Servidores de Conteúdo × Notícias e Mídias × Organizações Políticas × Enciclopédias × Restaurante e Jantar × Sociedade e Estilo de Vida
Categoria Potencialmente Responsável	
Classificações Liberadas	**Classificações Bloqueadas**
	× Abuso de Criança × Discriminação × Abuso de Drogas × Violência Explícita × Grupo Extremista × Hacking × Ilegal ou Antiético × Plágio × Site de Proxy
Categoria Riscos de Segurança	
Classificações Liberadas	**Classificações Bloqueadas**
	× DNS Dinâmico; × Sites Maliciosos; × Domínios sem categorização; × Phishing; × Spam - URL´s; × Domínios recentemente registrados;
Sites sem Categorias e exceções	
Bloquear por padrão todos os sites sem categoria; Exceções deverão ser listadas e liberadas somente para esta categoria	

Referência: https://fortiguard.com/webfilter/categories