POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PROGUARU - PROGRESSO E DESENVOLVIMENTO DE GUARULHOS SA "em liquidação"

OBJETIVOS

Os objetivos desta Política são:

a) Delinear a forma de uso aceitável dos equipamentos, *softwares* e sistemas de informação da rede PROGUARU (PROGRESSO E DESENVOLVIMENTO DE GUARULHOS SA “em liquidação”).

b) Prover meios de proteger tanto os Acionistas, Conselheiros, Liquidante, membros da Comissão Liquidante, empregados, estagiários da PROGUARU e integrantes do quadro de pessoal de empresas contratadas, assim como os próprios recursos da PROGUARU, de ameaças, incluindo ataques de vírus, comprometimento da rede e dos serviços, e também quanto a questões legais.

c) Orientar sobre o uso, armazenagem e destruição de documentos contendo informações confidenciais, sejam relativas às pessoas ou relativas aos negócios da PROGUARU, bem como aos riscos associados ao uso e destruição inadequados desses documentos.

ABRANGÊNCIA

Esta política aplica-se aos Acionistas, Conselheiros, Liquidante, membros da Comissão Liquidante, empregados e estagiários da PROGUARU, incluindo integrantes do quadro de pessoal de empresas contratadas ou prestadoras de serviços, na condição de usuários dos recursos de TI (Tecnologia da Informação) ou de usuários das informações relativas a pessoas ou demais negócios da PROGUARU.

Aplica-se também a todos os equipamentos, *softwares* e aplicativos de propriedade de empresas que estejam alocados nas dependências da PROGUARU em caráter de demonstração, homologação, testes ou efetiva utilização.

ÁREA GESTORA

Cabe à Seção de Informática, subordinada ao Departamento de Planejamento e Administrativo da PROGUARU, a gestão do conteúdo relativo à segurança da informação, assim como definir diretrizes e orientações estratégicas relacionadas ao tema.

SUMÁRIO

1. INTRODUÇÃO GERAL

As normas aqui descritas estão segmentadas em dois tópicos:

a) **Segurança e uso responsável de recursos de TI -** Apresenta as normativas de uso dos recursos de Tecnologia de Informação da PROGUARU, visando a preservação da Segurança de Informações e da integridade dos mesmos.

b) **Segurança de documentos** - Disciplina o uso da informação dentro da PROGUARU, preservando o sigilo das pessoas e de informações internas consideradas como estratégicas.

2. SEGURANÇA E USO RESPONSÁVEL DE RECURSOS DE TI

Esta Política fornece orientação e regras para a promoção do uso adequado e responsável dos recursos de TI da PROGUARU, com o intuito de prover meios para proteger nossos usuários e a própria instituição de ações ilegais ou danos que possam ser perpetradas por pessoas internas ou externas à organização, sejam estas ações intencionais ou acidentais.

2.1. Definições

Neste documento serão utilizados alguns termos técnicos e expressões, os quais podem não ser de conhecimento imediato dos usuários.

Consideram-se como recursos de TI qualquer item considerado, mas não limitado, às descrições abaixo:

Hardware	Conjunto de componentes físicos de um equipamento com capacidade de processamento de informações
Microcomputador	Equipamento de pequeno porte utilizado para execução de programas
Servidor	Equipamento central de média ou grande capacidade de processamento dedicado ao processamento de informações corporativas
Roteadores	Equipamentos especializados para controle de redes locais
Switches	Equipamentos especializados para controle de redes locais

Firewalls	Equipamento dedicado a funções de segurança de rede
IDS	Detector inteligente de acesso à Internet
Pendrives	Dispositivos móveis para armazenamento de informações
CD, DVD (R/RW)	Dispositivos móveis para armazenamento de informações
Mídias de armazenamento	Dispositivos dedicados ao armazenamento de informações. Ex.: *pendrives, CD e DVD (R/RW)*
Sistema Operacional	*Software*, ou um conjunto de *softwares*, que tem como papel gerenciar e administrar todos os recursos presentes em um sistema
Software	Programa ou conjunto de programas de um computador
E-mail	Programa de Correio eletrônico
Internet	Rede mundial de informações em computadores
Intranet	Rede interna de informações residentes em computadores
Contas de Rede	Credencial de usuário concedida pela área de TI
Browser	Programa especializado para acesso a informações da Internet ou Intranet
Telefones Digitais	Equipamentos de telefonia digital
Telefones Analógicos	Equipamentos de telefonia convencional
PABX	Central Telefônica Corporativa
Links de comunicação	Canais de comunicação entre pontos remotos
Leitores de *smartcard*	Equipamentos destinados à leitura de informações residentes em *chips* contidos em cartões
Impressoras	Equipamentos destinados à impressão de documentos
Tablets	Computadores portáteis de mão
Notebooks	Computadores portáteis
Rede Local	Conjunto de computadores interligados

2.2. Uso geral de recursos de TI

Os recursos de TI da rede PROGUARU, incluindo, mas não limitado a microcomputadores, servidores, equipamentos de segurança (*firewalls*), equipamentos de controle de rede local (roteadores, *switches*), impressoras, *softwares*, sistemas operacionais, mídias de armazenamento, contas na rede,

e-mail, acesso à Internet e Intranet, e telefonia devem ser utilizados estritamente para os fins a que se destina, no interesse da PROGUARU.

- Os usuários dos recursos de TI da PROGUARU são responsáveis pela utilização correta desses recursos, quando colocados à sua disposição, e também das informações neles disponibilizadas.
- As empresas que possuam profissionais alocados nas dependências da PROGUARU e que venham a ser usuários dos recursos de TI da PROGUARU devem prover orientações aos mesmos, previstas contratualmente, sobre o uso responsável dos recursos e das informações disponibilizadas pela PROGUARU.

Atualmente a PROGUARU possui uma rede *Wireless* (sem fio) desconectada da infraestrutura de rede local corporativa, e integrada à Internet, para que usuários específicos possam se beneficiar do uso de banda larga na navegação pela Internet e para o tratamento de seus *e-mails.*

2.3. Mecanismos de proteção dos recursos de TI

A PROGUARU considera como imprescindível o direito de proteger seus recursos de TI, desde equipamentos e *softwares* até as informações, tendo implantado as seguintes ferramentas e políticas:

a) os microcomputadores não possuem unidades de *CD (ROM ou RW), DVD (ROM ou RW)* e portas *USB* habilitadas, exceto o uso permitido e habilitado em situações excepcionais;
b) o acesso à rede local para um novo usuário é concedido pela Seção de Informática após processo de avaliação junto à área de atuação do usuário de acordo com a sua necessidade;
c) há uma política de concessão de direitos de acesso a informações das áreas, sendo de responsabilidade do gestor de cada área autorizar a concessão para cada tipo de acesso;
d) o acesso à Internet e correio eletrônico é monitorado por ferramentas de mercado, sendo de direito da PROGUARU, a avaliação do conteúdo das mensagens trafegadas na rede;

e) necessidades eventuais ou regulares de envio ou recebimento de informações em mídias de armazenamento deverão ser tratadas junto à Seção de Informática;
f) há também restrições quanto ao acesso de *sites* específicos e para a instalação de programas nos computadores;
g) a liberação de acesso extraordinário a *sites* específicos que estejam bloqueados na Internet ou instalação de programas é efetuada a partir de autorização da Seção de Informática por escrito (*e-mail* ou documentação), a partir de solicitação igualmente documentada;
h) as fronteiras entre os recursos de TI e o meio externo (Internet, conexão com outras empresas) são controladas e monitoradas por equipamentos de segurança (*Firewalls, IDS,* etc.);
i) estão instalados no servidor e nos computadores da PROGUARU, sistemas de detecção e combate a vírus e programas maliciosos (que tem como finalidade a exploração de informações confidenciais), com atualização automática contra novas ameaças;
j) as configurações do sistema operacional, residente nos computadores da PROGUARU, fornecem acesso limitado aos recursos dos equipamentos.

2.4. Condições de uso dos recursos de TI

As seguintes condições são consideradas como não autorizadas:

a) Violação de Propriedade Intelectual

- Utilizar ou divulgar material que viole direitos de propriedade intelectual de qualquer pessoa ou companhia, como marca registrada, nome comercial, segredo empresarial, domínio na Internet, patentes, desenho industrial ou qualquer outro material não autorizado expressamente pelo autor, que viole direito de propriedade industrial, artística ou literária.
- Instalar, distribuir ou utilizar *softwares* “pirateados” ou não licenciados para uso na PROGUARU.
- Fazer cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a: músicas, textos, digitalização e distribuição de

fotografias encontradas em revistas, livros ou em outras fontes protegidas por direitos autorais.

b) Manipulação não autorizada de informações e programas de computador

- Criar, transmitir, distribuir, colocar, armazenar ou tornar disponível através dos recursos da PROGUARU e da Internet qualquer material que viole leis ou regulamentações referentes à obscenidade, pornografia ou pedofilia; material que divulgue informações injuriosas, caluniosas ou difamatórias, que viole o direito à honra ou à imagem das pessoas; material que constitua ameaça a alguém; ou qualquer material que viole quaisquer leis e regulamentações vigentes.
- Divulgar informações confidenciais ou classificadas como estratégicas para a PROGUARU sob qualquer forma (*e-mail*, cópias, impressão, etc).
- Introduzir programas com códigos maliciosos na rede ou servidores (exemplo: vírus, *worms*, cavalos de troia, *spyware, phishing*).
- Divulgar informações de negócios, pessoais ou de empresas contratadas sem prévia anuência da Comissão Liquidante da PROGUARU.

c) Uso indevido de credenciais e senhas de acesso

- Divulgar códigos de identificação, autenticação e autorização de uso pessoal (conta de rede, senhas) ou permitir o uso por terceiros de recursos autorizados por meio dessas formas de acesso.
- Fornecer informações sobre funcionários ou lista de funcionários da PROGUARU a terceiros sem autorização expressa.
- Tentar se utilizar de relacionamentos pessoais, abuso de autoridade ou relação de confiança para obtenção de informações confidenciais ou credenciais de acesso a sistemas e infraestrutura não autorizados para o seu direito de acesso.

d) Violação de equipamentos

- Instalar ou tentar instalar nos computadores de propriedade da PROGUARU, unidades de mídia de armazenamento tais como, mas não limitados a

pendrives, discos rígidos, cartões de memória, ou quaisquer outros dispositivos de armazenamento interno ou externo.

- Conectar ou tentar conectar alguma forma de equipamento portátil tais como celulares, *tablets, laptops* e *notebooks* na rede local da PROGUARU.

e) Equipamentos

- Utilizar equipamentos pessoais (*notebooks*) nas dependências da PROGUARU, quer seja para desenvolvimento das funções profissionais ou para fins pessoais.

As exceções serão tratadas pela Comissão Liquidante da PROGUARU, devendo ser devidamente documentadas.

2.5. Acesso indevido à Internet e ao correio eletrônico

As seguintes condições são consideradas como não autorizadas:

a) Uso da Internet

Acessar *sites* na Internet cujo conteúdo seja considerado como impróprio para as suas funções na empresa, exceto situações especiais, e esteja classificado, mas não limitado, dentro das alternativas abaixo descritas:

- erótico ou pornográfico (de qualquer tipo);
- racismo e discriminação;
- militância política;
- ocultismo;
- difamação de entidades públicas ou privadas;
- esportes, apostas *on-line;*
- jogos *on-line;*
- conversação particular pela Internet (Microsoft Teams, Google Meet, Chats e assemelhados);
- *e-mail* particular (correio eletrônico em páginas na Internet);

- redes sociais pessoais (Facebook, Twitter, Facetime, WhatsApp e assemelhados);
- relacionados à prática ou estudo de formas de ataque à segurança de empresas, quer seja com objetivos de ganho financeiro ou não.

b) Correio eletrônico (*e-mail*) externo (Internet) e interno (Intranet)

- Utilizar recursos de *e-mail* para envio de *links* ou mensagens com conteúdo classificado como indevido ou não ético (pedofilia, pornografia, escárnio, ofensas aos bons costumes locais, cunho difamatório de qualquer espécie, correntes, apostas, entre outros).
- Utilizar recursos de TI da empresa para tráfego de mensagens instantâneas, comunidades virtuais na Internet ou na Intranet que não estejam diretamente relacionadas com o negócio da empresa e sem a prévia autorização da chefia imediata.
- Utilizar recursos de TI da empresa para repassar, internamente ou externamente, mensagens com conteúdo inadequado para a condução normal das atividades do usuário, como por exemplo, piadas, diversão, pornografia, esporte, escárnio.

2.6. Acesso indevido à rede de dados

As seguintes condições são consideradas como não autorizadas:

- Obter acesso não autorizado a dados, sistemas, redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades da rede, dispositivos da rede, ou violar a segurança ou medidas de autenticação, sem autorização expressa da Seção de Informática da PROGUARU.
- Efetuar monitoração não autorizada de dados ou tráfego em qualquer rede, sem a autorização expressa da Seção de Informática da PROGUARU.
- Executar qualquer forma de monitoramento da rede, o qual interceptará dados não destinados ao endereço do equipamento do usuário, a menos que essa atividade seja parte do trabalho normal do funcionário com a aprovação da Seção de Informática da PROGUARU.

- Fazer tentativas deliberadas para interferir em um serviço, sobrecarregar um serviço ou, ainda, tentar desativar um servidor, inclusive aderir a ataques de negação de serviços, quer seja para obter qualquer ganho como para testar a segurança da instituição.
- Utilizar comandos, *batches*, programas, *scripts* ou enviar mensagem de qualquer espécie com a intenção de interferir ou desabilitar uma sessão de usuário, via qualquer meio, localmente ou remoto.
- Obter acesso aos recursos da rede de informações (servidor, rede, conta de correio, sistemas ou aplicativos) sem a devida autenticação, através de meios fraudulentos.

2.7. Reprodução não autorizada de imagem e voz

- Efetuar qualquer tipo de reprodução de imagem (câmeras fotográficas ou câmeras embutidas em aparelhos celulares) em qualquer meio digital ou analógico dentro das dependências da PROGUARU sem prévia autorização.
- Utilizar qualquer recurso para reprodução de voz (celulares, gravadores, escutas telefônicas, captura de voz) em qualquer meio digital ou analógico dentro das dependências da PROGUARU sem prévia autorização.

2.8. Exceções

- Usuários da Seção de Informática, na execução de suas responsabilidades, poderão estar isentos dessas restrições (administradores de redes), desde que previamente autorizados pelo Departamento de Planejamento e Administrativo, e estarão autorizados a interferir nos acessos de equipamentos se estes estiverem afetando negativamente os serviços da PROGUARU.

Outras exceções serão tratadas pela Comissão Liquidante, devendo ser devidamente documentadas.

2.9. Monitoração de ocorrências e controles adicionais por parte da empresa

A PROGUARU reserva-se o direito de gravar as ligações de seus funcionários e colaboradores através de seus ramais telefônicos. Da mesma forma, são gravadas cópias das mensagens enviadas ou recebidas pelos funcionários através do sistema de correio eletrônico (*e-mail*).

O objetivo destas gravações é primordialmente fornecer subsídios para esclarecer dúvidas relativas a operações da empresa que tenham sido realizadas por telefone ou tenham tido detalhes informados via *e-mail*.

A PROGUARU reserva-se o direito de analisar o conteúdo destas gravações sempre que julgar necessário, com o intuito de assegurar-se da identificação da transmissão de informações classificadas como confidenciais ou estratégicas.

A divulgação de dados confidenciais ou estratégicos para terceiros ou estranhos às atividades funcionais, através de *e-mail* ou telefone é uma violação do Código de Conduta e Integridade da PROGUARU, caracterizando-se como falta grave, sujeitando as pessoas envolvidas às sanções decididas pela Comissão Liquidante da PROGUARU.

2.10. Recomendações importantes

Algumas recomendações são importantes para manter a segurança das informações da empresa e devem ser divulgadas:

- nunca discutir informações estratégicas em locais de circulação pública como corredores e áreas comuns da empresa;
- não deixar impressões de informações estratégicas da empresa em locais inadequados (impressoras, mesas, armários sem chave);
- não deixar nenhum material com informações pertinentes à empresa exposto em mesas, impressoras, *scanners* ou copiadoras;
- destruir por completo materiais com informações classificadas como confidenciais (estratégicas para os negócios da empresa) e que tenham de ser descartados, aproveitando-se os picotadores de papel existentes nas dependências da PROGUARU ou destruí-los manualmente;

- cartuchos de impressoras já usados devem ser recolhidos pela Seção de Informática, que providenciará o descarte junto ao fornecedor, nunca jogá-los em latas de lixo;
- não jogar mídias de armazenamento de informações no lixo sem antes destruí-las por completo;
- não efetuar mudanças de *layout* de recursos de TI, mas acionar a Seção de Informática da PROGUARU para tal mudança;
- não abrir nenhum *e-mail* que não se conheça a origem (remetentes não identificados ou suspeitos), que não declare o assunto ou que não possua relação com o trabalho do usuário;
- nunca executar programas ou tentar abrir *links*, imagens, vídeos, filmes ou qualquer outro conteúdo enviado por *e-mail* às caixas postais do usuário que sejam considerados suspeitos;
- nunca fornecer credenciais de acesso ou informações de *login* e senhas, ou dados pessoais (inclusive documentação) por *e-mail*, em *sites* na Internet ou ainda por telefone ou WhatsApp sem ter absoluta certeza da idoneidade do solicitante da informação;
- avisar a Seção de Informática da PROGUARU em casos de recebimento contínuo ou esporádico de *e-mails* onde não se conheça a origem ou com assunto estranho ao trabalho do usuário;
- sempre dar ciência à Seção de Informática ou Departamento de Planejamento e Administrativo sobre ocorrências de violações da Política de Segurança perpetradas por quem quer que seja, sendo que as informações prestadas serão tratadas com confidencialidade.

2.11. Ações de controle contra violações da Política de Segurança de recursos e medidas disciplinares

Caso ocorram violações a esta Política, a PROGUARU reserva-se o direito de adotar as medidas disciplinares que sejam cabíveis para o caso.

O conhecimento de uma violação desta Política por parte de funcionários ou prestadores de serviço e não informada à Seção de Informática ou Departamento de Planejamento e Administrativo da PROGUARU constitui falta grave passível de medidas disciplinares a serem tomadas contra o infrator.

A Seção de Informática da PROGUARU investigará as ocorrências de violação de segurança e poderá se envolver e cooperar na avaliação do dano, no caso de haver suspeita de violação que se caracterize como crime ou ação passível de sanção disciplinar.

Em casos de violação a esta Política, serão aplicadas as medidas disciplinares previstas no Código de Conduta e Integridade da Proguaru.

2.12. Política de senhas

- É de responsabilidade do usuário utilizar nome de usuário e senha, únicos e não compartilhados para acessar as informações e os sistemas da PROGUARU. As solicitações de alteração da senha deverão ser informadas à Seção de Informática.
- Evitar manter anotadas senhas, por exemplo, em papel, monitores, arquivos ou dispositivos móveis.
- Não armazenar senhas de forma desprotegida nos sistemas ou arquivos de um computador.
- Modificar senhas temporárias no primeiro acesso ao sistema.
- Não compartilhar senhas de usuários individuais.
- Os atos e atividades gerados pelo uso de um nome de usuário e senha são de responsabilidade do usuário.
- Considera-se fraude a tentativa por um usuário de quebrar ou descobrir a senha de um sistema ou de outros usuários.
- A desativação de uma conta de acesso poderá ser efetuada mediante a solicitação formal pela chefia imediata ou superior.
- Selecionar senhas de qualidade que atendam aos requisitos mínimos de segurança, conforme os seguintes critérios:
  a) ter no mínimo 8 caracteres;
  b) não ser igual às últimas 3 senhas cadastradas anteriormente;
  c) não possuir parte do nome do usuário;
  d) não ter sido alterada em período inferior a 24 horas da última redefinição;
  e) conter caracteres de pelo menos 2 grupos dos 3 relacionados abaixo:
     - maiúsculos (A a Z);
     - minúsculos (a a z);
     - dígitos de base 10 (números de 0 a 9);

f) caracteres não alfanuméricos (por exemplo: !, $, #, @, %, ., etc).

2.13. Normas gerais de *backup*

Definição de Objetivos:

- RTO (Recovery Time Objective): 4 horas
- RPO (Recovery Point Objective): 96 horas

a) Seleção de Soluções de *Backup*:

- *Software* de *backup: Cobian Backup*
- *Hardware* de armazenamento: Unidade de armazenamento em rede (NAS)

b) Políticas de *Backup*:

- realizar *backups* diários dos sistemas;
- realizar *backups* completos nos fins de semana;
- manter 90 dias de retenção de *backup* local.

c) Calendário de *Backup*:

- segunda à sexta-feira: *Backup* incremental dos sistemas a cada 2 horas;
- sexta-feira: *Backup* completo dos sistemas e dados às 21h.

d) Testes de Recuperação:

- realizar testes de recuperação mensalmente para garantir a eficácia dos *backups.*

e) Armazenamento Seguro:

- manter o NAS em uma sala segura e protegida contra acesso não autorizado;

- armazenar *backups* em nuvem em uma conta segura com autenticação de dois fatores.

3. SEGURANÇA DE DOCUMENTOS

Todas as instituições têm o dever de zelar pelo sigilo dos dados apresentados por seus usuários.

O presente documento apresenta orientações sobre como classificar um documento, em função da informação nele registrada, além de orientações sobre a custódia desta informação e meios a serem utilizados para destruição de informações classificadas como confidenciais.

Parte das informações aqui apresentadas encontra-se registradas no Código de Conduta e Integridade da PROGUARU, disponibilizado a todos os funcionários no Portal da Transparênica.

3.1. Classificação de Informações

Toda informação pode ser classificada em níveis de confidencialidade, dependendo da importância da informação e dos riscos associados à uma eventual divulgação indevida.

Abaixo segue uma recomendação para a classificação do grau de confidencialidade das informações:

a) **Não Classificadas** – Informações de uso geral, que não comprometam a PROGUARU e possam ser divulgadas internamente sem causarem impacto negativo aos negócios da empresa.

b) **Uso Interno –** Informações cuja divulgação possa ser inconveniente ou inapropriada, pois trata de assuntos exclusivamente internos.

c) **Divulgação Restrita** – A divulgação destas informações pode causar problemas ou prejuízos à PROGUARU.

d) **Confidencial** – Informações cuja divulgação possam causar sérios problemas. **Todas as informações relativas a pessoal ou estratégias da empresa são classificadas como confidenciais.**

O uso do bom senso é fundamental para avaliar o grau de confidencialidade das informações, entretanto os funcionários devem discutir o assunto com seus gestores sempre que surgirem dúvidas, antes de qualquer divulgação.

3.2. Utilização de Informações

É vedada a divulgação externa de informações, classificadas como confidenciais, recebidas pelos funcionários da PROGUARU, devendo obedecer estritamente às instruções de compartilhamento das mesmas.

É importante lembrar que vários funcionários da PROGUARU têm também acesso a dados reservados dos fornecedores e prestadores de serviço como endereço, dados pessoais, contato telefônico, etc. As informações pessoais são protegidas por lei e devem ser tratadas com o rigor e cuidado necessário, de acordo com a Política de Privacidade e Proteção de Dados da Proguaru.

O descuido no tratamento destas informações poderá acarretar ao infrator medidas punitivas classificadas no Código Civil Brasileiro, na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados - LGPD e demais normativas relacionadas ao tema.

3.3. Proteção de Informações

Com o intuito de proteger a PROGUARU e seus colaboradores de eventuais vazamentos de informações, as seguintes orientações devem ser cumpridas por todos os funcionários, fornecedores e prestadores de serviço:

a) nunca imprimir um documento que contenha informações confidenciais, se não houver uma real necessidade;
b) caso a impressão deste documento seja realmente imprescindível, esse deverá ser mantido em ambiente seguro;
c) caso o documento não seja mais necessário, a informação impressa deverá ser destruída imediatamente;
d) os documentos impressos devem ser retirados das impressoras imediatamente, evitando o acesso a eles por outros funcionários;
e) todos os relatórios e outros documentos que não forem arquivados devem ser encaminhados para destruição;

f) cópias de documentos devem ser tratadas com o mesmo rigor que os documentos originais, ou seja, destinadas a um arquivo fechado ou à destruição;
g) documentos apresentados por funcionários (ex.: documentos pessoais, comprovante de residência) que não sejam utilizados para o fim específico, devem ser encaminhados para destruição após requisitos legais quanto ao tempo exigido no Decreto Municipal nº 25.624/2008, que dispõe sobre a Gestão de Documentos, os Planos de Classificação e a Tabela de Temporalidade de Documentos e define normas para avaliação, guarda e destinação de documentos de arquivo no município de Guarulhos;
h) todos os setores da PROGUARU que lidam com informações confidenciais devem preferencialmente utilizar equipamento para fragmentar papéis. Em caso de ausência desse equipamento, deve ser providenciada a destruição manual e completa dos documentos a serem inutilizados;
i) documentos ou cópias de documentos não devem ser jogados em cestos de lixo comum em hipótese alguma, devendo ser destruídos e descartados;
j) os armários onde são arquivados documentos confidenciais devem ser mantidos trancados durante todo o tempo;
k) as gavetas de mesas devem ser mantidas fechadas à chave, caso contenham documentos ou informações internas, restritas ou confidenciais.

O não cumprimento dessas orientações, quando do tratamento de informações concernentes à PROGUARU, poderá acarretar ao infrator medidas punitivas classificadas no Código Civil Brasileiro, na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados - LGPD e demais normativas relacionadas ao tema.

3.4. Mesas Limpas

Por questão de segurança da informação, não deve ser deixado sobre a mesa de trabalho nenhum documento confidencial que não seja utilizado imediatamente. Documentos soltos sobre a mesa de trabalho podem ser extraviados facilmente ou ter suas informações acessadas por outras pessoas.

A PROGUARU determina que informações não divulgadas publicamente devam ser protegidas adequadamente, visando o cumprimento da legislação e regulamentação aplicáveis.

3.5. Ações de controle contra violações da Política de Segurança de documentos e medidas disciplinares

As ações contra as violações a esta Política e medidas disciplinares a serem aplicadas são as mesmas descritas no item 2 - Segurança e Uso Responsável de Recursos de TI.

4. GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

O objetivo desta Política também é assegurar que incidentes ou possíveis incidentes de violação de dados pessoais sejam resolvidos de forma efetiva, com a prioridade adequada, permitindo o registro, a investigação e a tomada de ação corretiva em tempo hábil para mitigar o impacto negativo junto aos titulares dos dados pessoais, preservando a imagem da PROGUARU e seu comprometimento com a proteção de dados pessoais.

Os incidentes de violação de dados pessoais devem ser prevenidos pela PROGUARU por meio da fiscalização da conformidade, com base nas normas legais e internas, especialmente as Políticas de Segurança da Informação e de Privacidade e Proteção de Dados.

Os usuários da PROGUARU devem ser capazes de prevenir e detectar um incidente de violação de dados pessoais, bem como estar aptos a promover as medidas de resposta adequadas conforme o caso.

Todo usuário que identifique um possível incidente de violação de dados pessoais deve comunicar imediatamente ao gestor de seu Departamento, cabendo a este comunicar ao Encarregado da Proteção de Dados Pessoais.

O Encarregado de Proteção de Dados Pessoais da PROGUARU, ao receber a comunicação de um possível incidente, ou, de ofício, deve:

a) avaliar o tipo e o nível de risco da violação de dados;
b) registrar o incidente;
c) determinar se o incidente acarreta risco para os direitos dos titulares dos dados pessoais, conforme definição da LGPD.

O risco deve ser avaliado de forma objetiva, conforme descrito na Política de Gestão de Riscos da PROGUARU.

Observado o nível de risco, o Encarregado de Proteção de Dados Pessoais da PROGUARU deve notificar a ocorrência do incidente à ANPD e aos titulares dos dados pessoais envolvidos.

REFERÊNCIA BIBLIOGRÁFICA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

Declaração

Declaro estar ciente da Política de Segurança da Informação definida neste documento e comprometo-me a cumprir as normas por ela detalhadas, sendo inteiramente responsável pela minha conduta na utilização dos recursos de Tecnologia da Informação e das informações disponibilizadas pela PROGUARU para a execução das minhas funções profissionais.

Também estou ciente de que a PROGUARU reserva-se o direito de analisar o meu acesso à Internet assim como o conteúdo das mensagens transmitidas via correio eletrônico ou os registros de ligações telefônicas, com o intuito de ser preservada a segurança e privacidade de suas informações.

Declaro, ainda, que estou ciente de que os equipamentos utilizados na criação e leitura das informações são de propriedade da PROGUARU, pelo que a leitura do respectivo conteúdo pela PROGUARU não configura violação de correspondência.

Nome Completo: _____

Matrícula: _____

Empresa (se terceiro): _____

Data: ___ /____/_____

Assinatura: _____