Política de Segurança da Informação

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 |RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

Sumário

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

Documento	Política
Classificação	Restrito/Interna
Elaboração	TI – Tecnologia da Informação
Aprovação	INTERV – Interventor
Vigência	Indeterminada, a partir da data de aprovação.
Revisado em	31/07/2024
Versão	3.0
Emissão	Israel da Silva Leite Junior

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

Legislação, normativos e referências

Abaixo encontra-se uma lista não exaustiva de normativos e referências relevantes para esta Política.

Lei Complementar nº 108/2001

Lei Complementar nº 109/2001

Resolução CGPC nº 13/2004

ISO/IEC 27002:2005

Associação Brasileira de Normas Técnicas - http://www.abnt.org.br/

International Organization for Standardization - http://www.iso.org/iso/home.html

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - http://www.cert.br

Tribunal de Contas da União - http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF

SENAC / SP - http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf

IMA - http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao

IPHAN - http://www.iphan.gov.br/baixaFcdAnexo.do?id=4010

ABRAPP – Manual de Boas Práticas em Tecnologia da Informação

Governança de TI – Peter Weil / Jeanne W. Ross

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

I. Introdução

A política de segurança da informação, também conhecida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da SWOTGLOBAL para proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada por todas as áreas do Instituto.

A presente PSI está baseada nas recomendações proposta pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de práticas para gestão da Segurança da informação, estando também de acordo com as leis vigentes em nosso país.

II. Objetivos

Estabelecer diretrizes que permitam a todos os colaboradores e prestadores de serviços da SWOTGLOBAL seguirem os padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócios e à proteção legal da empresa 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 da SWOTGLOBAL 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.

III. Público Alvo

Entende-se como público alvo desta política:

- **Colaboradores:** entende-se por colaborador toda e qualquer pessoa física, contratada CLT, mesmo os em regime temporário de contratação, ou prestadora de serviço por intermédio de pessoa Jurídica ou não, que exerça alguma atividade dentro ou fora da Instituição.
- **Prestadores de serviços:** entende-se como prestador de serviços o profissional que trabalha sem vínculo empregatício. Portanto, suas obrigações e direitos não se baseiam na CLT. Desse modo, as questões referentes a execução do serviço são negociadas livremente entre o prestador e a empresa contratante e firmados via assinatura de contrato.

IV. Aplicações da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, e prestadores de serviços; e se aplicam a informações em qualquer meio ou suporte.

Esta política dá ciência a todos de que os sistemas, computadores e redes da empresa poderão ser monitorados e gravados, conforme previsto nas leis brasileiras vigentes.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de

Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

V. Princípios da PSI

Toda informação produzida ou recebida como resultado da atividade profissional contratada pelo SWOTGLOBAL Instituto de Seguridade Social, pertence à referida Instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação deverão ser utilizados exclusivamente para a realização das referidas atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas de serviços e mediante prévia autorização do gestor direto.

O SWOTGLOBAL, por meio da área de Tecnologia da Informação (TI), poderá registrar todo o uso dos sistemas, visando garantir a disponibilidade e a segurança das informações utilizadas.

VI. Requisitos da PSI

Para a uniformidade da informação, deverá ser dada ciência a todo o público alvo desta política do SWOTGLOBAL, 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 correlatas deverão ser revistas e atualizadas, sempre que algum fato relevante ou evento motive sua revisão.

Deverá constar em todos os contratos do SWOTGLOBAL uma cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela Instituição.

No momento da contratação, ou seja, em quaisquer relações de trabalho, deve ser firmada a assinatura do Termo de Ciência e Responsabilidade desta PSI atestando a responsabilidade quanto ao cumprimento das regras descritas neste normativo e suas responsabilidades para com a Proteção de Dados Pessoais.

Todos os definidos no público alvo desta política devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

Para os contratados em período anterior à publicação desta política, e que não tenham assinado os respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI, juntamente com este normativo para a respectiva assinatura de forma física ou eletrônica.

Cabe a área administrativa colher a assinatura e arquivar o Termo de Ciência e Responsabilidade da PSI dos profissionais já contratados.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à TI cabendo a mesma, se julgar necessário, encaminhar posteriormente à gerência responsável e ao comitê de segurança da informação.

O SWOTGLOBAL exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos colaboradores e prestadores de serviços, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, podendo adotar as medidas legais cabíveis. O não cumprimento dos requisitos previstos nesta PSI acarretará violação às regras internas da Instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

A. Dos Colaboradores em Geral

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

Nenhum computador do instituto poderá ser alterado de lugar ou posição, a não ser que seja acompanhado por um responsável da área de informática. *Notebooks* somente poderão ser solicitados para serviços externos quando justificados os serviços a ser realizados, com autorização do superior hierárquico, salvo quando observadas as regras definidas na modalidade de *Home Office*.

B. Dos Colaboradores em Regime de Exceção (Temporários)

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

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

C. Dos Gestores de Pessoas (RH)

Atribuir a todos abrangidos por esta política na fase de contratação e de formalização dos contratos de trabalho, de prestação de serviços ou de parceria, a responsabilidade pelo cumprimento da PSI do SWOTGLOBAL.

Garantir a assinatura do Termo de Ciência e Responsabilidade da PSI, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os acessos as informações da SWOTGLOBAL.

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.

Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

D. Dos Custodiantes da Informação

Competem aos custodiantes das informações as seguintes atribuições:

- Testar a eficácia dos controles utilizados e informar aos gestores e ao comitê de segurança da informação os riscos residuais;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de respostas 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 complementares;
- Garantir, após solicitação formal, o bloqueio de acesso de usuário por motivos de desligamento do Instituto, incidentes, 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 relógio de sincronizado com os servidores de oficiais do governo brasileiro;

- Monitorar todos os ativos de informação da empresa contra códigos maliciosos, e garantir que os novos ativos só entrem para o ambiente de produção da empresa em processo de mudança, sendo ideal a auditoria de códigos e a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Garantir o levantamento de todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, identifica-los durante a definição de escopo de um projeto ou sistema; seja justificando ou documentando, implantado e efetuando testes durante a fase de execução.;

Os operadores com perfil de administradores 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 execução de atividades operacionais sob sua responsabilidade como, por exemplo, manutenção de computadores, realização de cópias de segurança, auditorias e teste de ambiente, desde que respeitados os critérios técnicos atribuídos a área de TI.

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 sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário, ou então fazer um backup das informações.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, base de dados e qualquer outro ativo de informação a um responsável pessoa física.

E. Da área de Segurança de Informação

São atribuições:

- Propor as metodologias e os processos específicos para segurança da informação, tais como avaliação de risco e sistema de classificação da informação;
- Propor e apoiar iniciativas que visem à segurança dos acessos de informações do Instituto;
- Publicar e promover as versões da PSI e aprovadas pelo Comitê de Segurança da Informação;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Analisar criticamente incidentes em conjunto com a gerência responsável pela segurança da informação;
- Manter comunicação efetiva com a gerência responsável sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o SWOTGLOBAL;
- Manter o acesso restrito à navegação de internet, para diminuir o risco de contaminação da rede por vírus, trojans, furtos e etc;
- Propor investimento relacionados à segurança da informação com objetivo de reduzir mais os riscos;
- Propor alterações nas versões da PSI e inclusão, eliminação ou mudança das normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir junto à Gerência responsável as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas da Segurança da Informação complementares.

F. Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, a SWOTGLOBAL 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 eventual material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, com solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- realizar, a qualquer tempo, inspeção física nas máquinas da SWOTGLOBAL;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
  - uso de capacidade instalada da rede e dos equipamentos; o tempo de resposta no acesso à internet dos sistemas críticos da SWOTGLOBAL;
  - período de indisponibilidade no acesso à internet e aos sistemas críticos da SWOTGLOBAL;
  - incidente de segurança (vírus, trojans, furtos, acessos indevidos, assim por diante);
  - atividades de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mail recebidos/enviados, *upload/download* de arquivos, entre outros);

VII. Correio Eletrônico

Destina-se a o uso de correio eletrônico da SWOTGLOBAL para fins corporativos e relacionados às atividades do colaborador dentro da instituição. A utilização desse serviço para

fins pessoais é permitida desde que feita com bom senso, desde que não prejudique a SWOTGLOBAL e também não cause impacto no tráfego da rede.

É proibido aos usuários produzir, transmitir ou divulgar mensagem que:

- Usem do correio eletrônico da SWOTGLOBAL para enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Instituição;
- Usem o nome de outro usuário ou endereço de correio eletrônico que não o seu individual;
- Que tornem seu remetente e/ou a SWOTGLOBAL ou suas unidades vulneráveis a ações civis ou criminais;
- Divulguem informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Visem burlar as informações de endereçamento, adulterar cabeçalho para esconder a identidade de remetente e/ou destinatário, com o objetivo de evitar punições;
- Apaguem mensagens de correio eletrônico quando qualquer uma das unidades da SWOTGLOBAL estiver sujeita a algum tipo de investigação;
- Contenham qualquer ato ou forneça orientação que conflite ou contrarie os interesses da SWOTGLOBAL.
- Contenham ameaças eletrônicas, como: spam, mail *bombing*, vírus de computador.
- Contenham arquivo com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente risco à segurança;
- Visem obter acesso não autorizado a outro computador, servidor ou rede;
- Visem interromper um serviço, servidores ou rede de computador por meio de qualquer método ilícito ou não autorizado;
- Visem burlar qualquer sistema de segurança;
- Visem vigiar secretamente ou assediar outro usuário;
- Visem acessar informações confidenciais sem explícita autorização do superior hierárquico, com o “De Acordo” do DPO. proprietário ou de coordenador responsável por escrito; TI

- Visem acessar indevidamente informações que possam causar prejuízo a qualquer pessoa;
- Tenha conteúdo considerando impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;
- Contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental e etc.;
- Tenham fins políticos.

No âmbito das atribuições da área de TI nos casos de desligamento de colaborador, deve ser observada a seguinte regra:

A conta de e-mail do colaborador desligado não poderá ser apagada, o e-mail permanecerá ativo por até 90 dias quando será desabilitado. Neste período o sistema identificará e-mails recebidos neste período e emitirá e-mail resposta automática informando que o colaborador não pertence mais ao quadro de colaboradores da SWOTGLOBAL, informando novo direcionamento; para não se perder as informações do e-mail um *backup* será feito, e disponibilizado para consultas quando necessário.

As mensagens de correio eletrônico dos colaboradores sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Cargo
- Telefone(s)
- Correio eletrônico
- Endereço

VIII. Internet

Todas as regras atuais da SWOTGLOBAL visam basicamente ao 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 o acesso das informações.

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

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

A SWOTGLOBAL, 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 autorização para tanto, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

O uso de qualquer recurso em atividades ilícitas poderá acarretar sanções administrativas, penais e cíveis sendo que nesses casos, a instituição cooperará ativamente com as autoridades competentes.

Aos usuários é permitido:

- Usar a internet disponibilizada pela instituição, independentemente de sua relação contratual, para fins pessoais, desde que não prejudique o andamento dos trabalhos;
- Fazer *download* (baixar) somente de programas ligados diretamente às suas atividades no instituto e, mesmo assim, sendo acompanhada por um responsável da área de TI;
-

- Serviços de comunicação instantânea (*SKYPE e WhatsApp Web*), mediante solicitação formal de acesso ao setor da TI e autorização expressa do Diretor Presidente da entidade.

Quanto as vedações:

- usar, instalar, copiar ou distribuir de forma não autorizada: *softwares* que tenham direitos autorais, marca registrada ou patentes na internet. (Qualquer software baixado, que não tenha sido autorizado, será excluído pela TI);
- utilizar os recursos da SWOTGLOBAL para fazer *download* ou distribuição de *softwares* ou dados pirateados, atividade está considerada delituosa de acordo com a legislação nacional;
- utilizar os recursos da SWOTGLOBAL para deliberadamente propagar qualquer tipo de vírus, *worm,* cavalo de troia, *spam*, para fins de assédio, perturbação ou controles de outros computadores;
- Acessar a softwares *peer-to-peer* (*Kazaa, BitTorrent* e afins).
- Não é permitido, em hipótese alguma, acesso a sites de proxy[1]

IX. Identificação

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

Todo os dispositivos de identificação utilizados na SWOTGLOBAL, como o número de registro, crachá, identificações de acesso ao sistema, certificados e assinaturas digitais e dados

[1] **Proxy** é um serviço que age como como intermediador entre usuário e a internet. Ele recebe e repassa todas as requisições ao site que você está acessando e o IP registrado nessas páginas acessadas é o do *proxy* e não o seu. Assim, sua identificação não fica exposta na rede, dificultando que você seja rastreado.

biométricos devem de estar associados a uma pessoa física e atrelados inequivocamente a seus documentos oficiais reconhecidos pela legislação brasileira.

Os dispositivos de identificação e senha protegem a identidade dos usuários, evitando e prevenindo que uma pessoa se faça passar por outra perante a SWOTGLOBAL e/ou terceiros.

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

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

O uso dos dispositivos e/ ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art .307 – falsa identidade), caso constatado o uso compartilhado a responsabilidade perante à SWOTGLOBAL e à legislação (cível e criminal) será dos usuários que dele se utilizarem.

A administração é responsável por passar informações do usuário para o setor de TI, para que possa ser feito uma criação de identidade lógica, bem como dos termos do procedimento para gerenciamento de conta de grupo e Usuários estes informados pela Gerencia onde será lotado o usuário.

Devem ser distintamente identificados quaisquer tipos de usuários dos sistemas, sejam eles pessoas físicas e/ ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a senha conforme as orientações apresentadas.

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

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre 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.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para desbloqueio é necessário que o usuário entre em contato com TI da SWOTGLOBAL.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido a seu login/senha.

A periodicidade máxima para troca das senhas é de 90 (noventa) dias, não podendo ser repetida as 3 (três) últimas senhas.

Comunicar formalmente e imediatamente à TI toda e qualquer alteração no quadro funcional do Instituto, tais como: contratações, demissões, alterações de cargos, funções, entre outros, no prazo mínimo de 24 horas, e de imediato em casos específicos (demissões/encerramento de contratos), a fim de evitar acessos não autorizados e/ou desnecessários.

Todos os acessos devem ser imediatamente bloqueados nos casos em que usuário for demitido ou solicitar demissão, férias, afastamento por motivos de saúde, o departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao departamento de TI, a fim de que essa providência seja tomada. Excetuam-se dos casos acima os gestores das áreas, salvo em casos de demissão. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à TI responsável para cadastra uma nova.

X. Computadores e Recursos Tecnológicos

Os equipamentos são disponibilizados pela SWOTGLOBAL, e cabem a cada usuário utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir os procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um analista da área de Tecnologia da Informação da SWOTGLOBAL, ou de quem este determinar.

As gerências que necessitarem realizar aquisição de sistemas e máquinas, deverão solicitá-los previamente à TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o setor técnico responsável mediante a *e-mail*.

A transferência e/ou a divulgação de qualquer *software*, programa ou instruções de computador para terceiros, por qualquer meio de transporte físico ou lógico, (programas de acesso remoto exemplo: *ANYDESK*), 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 de destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da SWOTGLOBAL (fotos, músicas, vídeos, etc...) não poderão 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 driver C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os usuários dos sistemas 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 TI.

Todas as alterações, compras e implantações de sistemas deverão ter anuência da área de TI.

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

- Nenhum dispositivo estranho pode ser conectado ao seu computador, quando for necessário, a TI deve ser informada para análise do dispositivo e autorização da conexão, caso concorde com o procedimento;
- 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 TI do SWOTGLOBAL ou por terceiros devidamente contratados para o serviço;
- Todos os modens internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informação, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante autorização do Gerente da área responsável;
- É expressamente proibido o consumo de alimentos, bebidas na mesa de trabalho e próximo aos equipamentos;
- O usuário deverá manter a configuração do equipamento conforme disponibilizado pela SWOTGLOBAL, seguindo os devidos controles de segurança exigidos pelo Política de Segurança da Informação e pelas normas especificas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueadas), nos padrões de protocolos de autenticação da ferramenta *Active Directory*, configurada no servidor;
- Todos os recursos tecnológicos adquiridos pelo instituto devem ter imediatamente suas senhas padrões (*default*) alteradas;
- Os equipamentos deverão ser preservados de modo seguro;
- Os computadores sempre deverão ser desligados após o encerramento do expediente. O usuário será notificado, via e-mail pelo setor da TI, caso o ocorrido se

repita por mais de 3 (três) vezes. A TI encaminhará o ocorrido para a gerência direta para as devidas providências; salvo em casos excepcionais mediante comunicação prévia.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da SWOTGLOBAL.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou *software*, como por exemplo, analisadores de pacotes (*sniffers*);
- Interromper serviço, dos servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- 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 propriedade intelectual, sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, e a ordem pública.
- Utilizar *software* pirata, atividade considerada delituosa de acordo com legislação nacional.

XI. Dispositivos Móveis

A SWOTGLOBAL deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores e prestadores de serviços. Por isso, permite que eles usem dispositivos móveis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua TI, como: *notebooks, Tablets,* HDs e ou mídias de armazenamento externos.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos que utilizem tais equipamentos.

A SWOTGLOBAL, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de monitorar e inspecioná-los a qualquer tempo, caso seja necessário realizar manutenção de segurança.

Os colaboradores e prestadores de serviço, portanto, assumem os seguintes compromissos:

- não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SWOTGLOBAL, mesmo depois de terminado o vínculo contratual mantido com a instituição;
- não realizar em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial à referente à segurança e à geração de logs, sem a devida comunicação e autorização da área responsável, bem como sem a condução, auxílio ou presença de um técnico da TI;
- não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da TI da SWOTGLOBAL;
- notificar o instituto em caso de furto ou roubo de um dispositivo móvel fornecido pela SWOTGLOBAL, registrando, assim que possível, um boletim de ocorrência (BO).

Todos abrangidos por esta política deverão:

- Realizar periodicamente cópias de segurança (*backups*) dos dados de seu dispositivo móvel;
-

- Manter esses *backups* separados de seu dispositivo móvel, ou seja, não os carregar juntos;
- Utilizar senhas de bloqueio automático para seu dispositivo móvel.

O suporte técnico aos dispositivos móveis de propriedade da SWOTGLOBAL e aos seus usuários deverão seguir os mesmos fluxos de suporte adotados pela instituição.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador, como: sua casa, hotéis, fornecedores e clientes.

Este normativo da ciência a todo o público alvo de que o uso indevido do dispositivo móvel caracterizará assunção (aceitação, concordância, assumir) de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venham causar à SWOTGLOBAL e/ou a terceiros, sendo passível de sanções administrativas quando necessário.

Equipamentos portáteis, como *smartphones, palmtops*, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão na rede corporativa.

Em casos excepcionais os equipamentos citados no item anterior quando necessária sua utilização deverá ser submetida previamente ao processo de autorização e validação da área de TI.

XII. Backup

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executadas fora do horário comercial, nas chamadas "janelas de *backup*" – período em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

As mídias de *backup* (como DAT, DLT, LTO, DVD, CD, HD e outros) devem ser acondicionadas em local seco, climatizado, seguro.

O tempo de vida e uso das mídias de *backup* devem ser monitorados e controlados pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além dos acompanhamentos dos prazos recomendados pelo fabricante.

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

Será realizado backup diário e mensal de todas as pastas, menos das pastas "público" e *"scanner".*

Os dados contidos na pasta público serão removidos periodicamente toda segunda-feira.

XIII. Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SWOTGLOBAL. Ou seja, qualquer incidente de segurança assemelha-se a alguém agindo contra a ética e os bons costumes regidos pela Instituição.