PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Normas e Diretrizes Administrativas

"Todo colaborador que fará uso dos recursos computadorizados da UPDI / Teleglobe, tem o dever e a responsabilidade de zelar pela segurança e a integridade das informações e dos equipamentos de informática" - Comitê de Segurança da Informação

Esta PSI tem como base e referencia:

- *LEI 13.709 / 18 – Lei Geral de Proteção de Dados Pessoais (LGPD)*
- *Norma ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação*

HISTÓRICO DE VERSÕES:

Versão 1.0

Criação: Thiago Bagnoli Moretti / Paulo Alberto Werhli Meier

Aprovação: Comitê de Segurança da Informação

Revisão 1.1: Thiago Bagnoli Moretti

SUMARIO

APRESENTAÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes da **UPDI / Teleglobe** 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 empresa. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001, 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.

1-OBJETIVOS

1.1- Estabelecer diretrizes que permitam aos colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de 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. Garante a proteção das informações entre clientes e empresa quanto à:

a) **Integridade:** garantia de que a informação seja mantida em seu estado original não sendo adulterada falsificada ou furtada, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
b) **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
c) **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

1.2- A PSI aplica-se a todos os colaboradores da empresa e a qualquer pessoa detentora de informações, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte

1.3- Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais, (Lei nº 9610).

2-REQUISITOS DA PSI

2.1- Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da UPDI / Teleglobe a fim de que a política seja cumprida dentro e fora da empresa.

2.2- Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como **Comitê de Segurança da Informação (CSI)**.

2.3- A PSI deverá ser revista e atualizada periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

2.4- A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar uma cópia desta PSI e, a cada mudança, além da nova ciência, deverão assinar novamente.

2.5- Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Supervisão, conforme a cadeia hierárquica, e se este julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

2.6- Deverão ser criados e instituídos controles apropriados, como registros de atividade (logs), em todos os pontos e sistemas em que a empresa 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 e nos sistemas.

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

2.8- A UPDI / Teleglobe exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, 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.

2.9- Esta PSI é obrigatória para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

2.10- O não cumprimento dos requisitos previstos nesta PSI acarretará violação às regras internas e sujeitará o usuário às medidas administrativas e legais cabíveis.

2.11- 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.

3-DAS RESPONSABILIDADES ESPECÍFICAS

3.1 - Dos Colaboradores em Geral

3.1.1- 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 empresa.

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

3.2 - Dos Detentores da Informação

3.2.1 - Da Área de Tecnologia da Informação

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

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

3.2.1.3- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

3.2.1.4- Os administradores do sistema podem, pelas características de seus privilégios, 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 testes entre outros.

3.2.1.5- Segregar as funções operacionais 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.

3.2.1.6- 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.

3.2.1.7- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes.

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

3.2.1.9- 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.

3.2.1.10-Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida.

3.2.1.11-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:

a) Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
b) Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

3.2.1.12-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.

3.2.1.13-Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança.

3.2.1.14-Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

3.2.1.15-Realizar auditorias periódicas de configurações técnicas e análise de riscos.

3.2.1.16-Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais, caso tenha autorização para tal.

3.2.1.17-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.

3.2.1.18-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.

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

a) Tempo de resposta no acesso à internet e aos sistemas críticos;
b) Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

3.2.2 - Da Área de Segurança da Informação

3.2.2.1- 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 da empresa.

3.2.2.2- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio.

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

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

3.2.3 - Do Comitê de Segurança da Informação

3.2.3.1- Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencia.

3.2.3.2- Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a empresa.

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

3.2.3.4 -Cabe ao CSI:

a) Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
b) Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
c) Avaliar os incidentes de segurança e propor ações corretivas;
d) Definir as medidas cabíveis nos casos de descumprimento da PSI;
e) Assessorar na implementação das ações de segurança da informação;
f) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

g) Propor Normas e Procedimentos internos relativos à segurança da informação em conformidade com as legislações existentes sobre o tema.
h) Sugerir ações visando ao alinhamento do plano de desenvolvimento de tecnologia da informação com o planejamento estratégico da empresa como um todo;
i) Apresentar sugestões e críticas com a finalidade de alinhar as áreas de negócio e todas as áreas envolvidas na disponibilização da infraestrutura tecnológica dos órgãos, no âmbito da Segurança da Informação;
j) Uniformizar as políticas de Segurança da Informação;
k) Elaborar a Política de Segurança da Informação e sua respectiva atualização;
l) Elaborar o Plano de Continuidade de Negócios, o Plano de Administração de Crises, Plano de Contingência, o Plano de Recuperação de Desastres e o Plano de Continuidade Operacional dentro do Programa de Gestão da Continuidade de Negócios além da sua respectiva atualização;
m) Analisar as necessidades em relação a Segurança da Informação;
n) Apreciar e emitir parecer sobre os relatórios das atividades desenvolvidas;

3.3 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

3.3.1- Para garantir as regras mencionadas nesta PSI, a UPDI/Teleglobe poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, 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;
b) Tornar públicas as informações obtidas pelos sistemas de monitoramento, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
c) Realizar, a qualquer tempo, inspeção física e/ou virtual nas máquinas de sua propriedade;
d) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

3.4 - DA MATRIZ DE ACESSO

3.4.1- Para que se cumpra de maneira efetiva, são efetuados mapeamento de logs e registros de acesso, que são conferidos periodicamente pelo Comitê de Segurança da Informação, afim de que se tenha Gestão de Identidades, Controle de Acessos, Revisões de Acessos, Controles de Vazamentos de informações e Prevenções de Fraudes.

3.4.2 - Os níveis de acessos ao sistema são distribuídos da seguinte forma:

a) NIVEL 3

Nível básico: é quem recebem as demandas de atendimento da empresa. É o primeiro contato do suporte, que pode ser realizado por chat, e-mail ou telefone. Se a demanda for de pouca complexidade, ele está apto a resolver. É responsável pelo atendimento e registro de todas as solicitações, direcionando os chamados para os níveis superiores. Os colaboradores que se enquadram neste nível, tem acesso limitado ao sistema, por este motivo, estão capacitados a resolver problemas de baixa complexidade, como configurações simples, com pequenas alterações, que podem ser feitas por ele ou orientadas aos clientes.

b) NIVEL 2

Nível Intermediário: destinado a questões mais técnicas e aprofundadas, como falhas mais complexas do software. Este nível é exercido por cargo de Supervisão, e é responsável por todos os chamados encaminhados pelo nível 3. Cabe a ele analisar os atendimentos com critérios técnicos e, estando fora dos seus níveis de acesso, repassar a demanda ao nível 1.

c) NIVEL 1

Nível máster: analisa problemas mais complexos do software, sendo exercido pelos cargos de Gerência. Atende a todos os problemas não solucionados pelos níveis anteriores. Possuem conhecimento amplo do software e tem acesso total ao sistema como um todo.

4-SEGURANÇA DA INFORMAÇÃO

4.1- O colaborador assume o compromisso de 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, mesmo depois de terminado o vínculo contratual mantido com a Empresa.

5-CORREIO ELETRÔNICO

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

5.2- O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador dentro da empresa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso e não prejudique ou cause impacto no tráfego da rede.

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

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

b) 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;
c) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a empresa vulneráveis a ações civis ou criminais;
d) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
e) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
f) Apagar mensagens pertinentes de correio eletrônico quando qualquer colaborador estiver submetido ou sujeito a algum tipo de investigação.
g) Produzir, transmitir ou divulgar mensagem que:

- ✓ Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da empresa;
- ✓ Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador, entre outros;
- ✓ Contenha arquivos com código executável 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;
- ✓ 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 e/ou mental entre 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.

5.3- As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

a) Nome do colaborador
b) Gerência ou departamento

c) Nome da empresa
d) Telefone(s)
e) Correio eletrônico

6-INTERNET

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

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

6.3- Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da UPDI / Teleglobe, 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.

6.4- A UPDI / Teleglobe, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

6.5- 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 empresa cooperará ativamente com as autoridades competentes.

6.6- A internet disponibilizada pela empresa aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

6.7- Como é do interesse da empresa 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.

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

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

6.10- O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

6.11- Os colaboradores não poderão em hipótese alguma utilizar os recursos para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

6.12- Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

6.13- Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

6.14- Os colaboradores não poderão utilizar os recursos da empresa para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, software para fins de assédio, perturbação ou programas de controle de outros computadores (exceto TeamViewer).

6.15- O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente.

6.16- Não é permitido acesso a sites de proxy.

7-IDENTIFICAÇÃO

7.1- Os dispositivos de identificação e senhas protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a empresa 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).

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

7.3- Todos os dispositivos de identificação utilizados, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e as assinaturas digitais têm de estar associadas a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

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

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

7.6- Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a UPDI / Teleglobe 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.

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

7.8- Serão distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas, mediante a apresentação de documento pessoal, bem como identificação da empresa. Este processo será realizado na portaria do edifício, e só terá o acesso as áreas restritas mediante autorização expressa.

7.9- Todo acesso de terceiros as áreas sensíveis e críticas, são acompanhadas pelo supervisor e / ou responsável do setor, desde a sua entrada até a sua saída, que será comprovada pela entrega do crachá na portaria.

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

7.11- 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.

7.12- 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.

7.13- Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Sistemas da Empresa.

7.14- Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

7.15- Cada colaborador possui um cartão Smart Card, com certificado digital pessoal, que deve ser inserido no leitor instalado em sua estação de trabalho. Os usuários não podem alterar a própria senha e, caso suspeitem que terceiros obtiveram acesso indevido a sua estação de trabalho, devem avisar imediatamente a Gerencia de Sistemas e, se for necessário, serão orientados a troca-la. A senha não pode ser igual as últimas 3 anteriores

7.16- Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas

7.17- O colaborador / usuário que, por descuido, perder, extraviar ou ainda, negligenciar a guarda do cartão, sofrerá as sanções definidas pela Gerencia de Sistemas, conforme a gravidade do seu ato.

7.18- Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

7.19- A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 45 dias.

7.20- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato à Gerencia de Sistemas, 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.

8-COMPUTADORES E RECURSOS TECNOLÓGICOS

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

8.2- A UPDI / Teleglobe, na qualidade de proprietário das estações de trabalho, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

8.3- 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 Sistemas, ou de quem este determinar. As gerências que necessitarem fazer testes, deverão solicitá-los previamente, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

8.4- Todas as atualizações e correções de segurança (patches) do sistema operacional ou aplicativos, somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois disponibilizadas no ambiente de produção.

8.5- No caso de ser identificado um patche critico, será dado a prioridade pela equipe responsável para que seja aplicado as devidas diretrizes, levando em consideração o tempo disponível para tal.

8.6- 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.

8.7- 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.

8.8- Arquivos pessoais e/ou não pertinentes ao negócio (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.

8.9- Documentos imprescindíveis para as atividades dos colaboradores da Empresa 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.

8.10- Os colaboradores 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 Sistemas.

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

a) Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
b) 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 Sistemas ou por terceiros devidamente contratados para o serviço.
c) O colaborador deverá manter as configurações do equipamento disponibilizado pela UPDI / Teleglobe, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação, assumindo a responsabilidade como custodiante de informações.
d) Todos os recursos tecnológicos adquiridos pela UPDI / Teleglobe devem ter imediatamente suas senhas padrões (default) alteradas.
e) Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

8.12- Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da UPDI:

a) Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
b) Burlar quaisquer sistemas de segurança.
c) Acessar informações confidenciais sem explícita autorização do proprietário.
d) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares.
e) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
f) 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;
g) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

8.13- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

9-DISPOSITIVOS MÓVEIS

9.1- A UPDI / Teleglobe deseja facilitar a mobilidade e o fluxo de informações entre seus colaboradores, permitindo o uso destes dispositivos, desde que não infrinjam as regras descritas nesta política.

9.2- Quando se descreve “dispositivos móveis” entende-se qualquer equipamento eletrônico com atribuições de mobilidade, aprovados ou não pela Gerência de Sistemas, como por exemplo, notebooks, smartphones, pendrives, câmeras fotográficas, entre outros.

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

9.4- O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Sistemas.

9.5- A reprodução não autorizada dos softwares instalados nos dispositivos móveis constituirá uso indevido do equipamento e infração legal.

9.6- O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a UPDI / Teleglobe e/ou a terceiros.

9.7- O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da empresa deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Sistemas.

9.8- No caso de trabalho remoto, serão gerados logs e trilhas para que sejam monitorados e apresentados, quando solicitados, a qualquer tempo. O acesso remoto só será possível se o colaborador estiver em posse de seu Smart Card.

10-DATACENTER

10.1- Todo acesso ao Datacenter pelo sistema (on-line), deverá ser registrado (usuário, data e hora) mediante software próprio.

10.2- A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

10.3- No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

11-TRILHAS DE AUDITORIA

11.1- As trilhas de auditoria (logs) são monitoradas e gravadas diariamente, sendo analisadas a cada 15 dias, gerando um relatório que será apresentado ao Comitê de Segurança da Informação, e aprovados por todos os membros.

11.2- Após a aprovação do relatório, as trilhas são arquivadas e segregadas de maneira física e logica, por um período de até 5 anos. Os relatórios aprovados pelo Comitê são devidamente arquivados.

12-BACKUP

12.1- Todos os backups devem ser automáticos por sistemas de agendamento automatizados 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.

12.2- 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.

12.3- 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.

12.4- 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.

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

12.6- 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.

12.7- Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

12.8- Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis.

12.9- Testes de restauração (restore) de backup devem ser executados por seus responsáveis, aproximadamente a cada 30 dias, de acordo com a criticidade do backup.

12.10- 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.

13-DAS DISPOSIÇÕES FINAIS

13.1- Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da UPDI / Teleglobe, sendo que todas as práticas que ameaçam a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até a rescisão contratual por justa causa, levando em consideração os fatores como: função exercida pelo colaborador, período da ocorrência, local, horário e prejuízo real ou potencial causado à UPDI / Teleglobe e seus clientes. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela empresa.