POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PO–005

SUMÁRIO

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

1. OBJETIVO

Apresentar um conjunto de regras para normatizar a segurança da informação e melhorar sua visão e atuação, buscando preservação das informações Comtex quanto a sua integridade, confidencialidade e disponibilidade.

2. SIGLAS E ABREVIATURAS

Sigla	Definição	Sigla	Definição
CAL	Controle e Avaliação da Legislação	**SGSI**	Sistema de Gestão de segurança da Informação
CPD	Centro de Processamento de Dados	**SGQSI**	Sistema de Gestão da Qualidade e Segurança da Informação
DHO	Desenvolvimento Humano Organizacional	**SI**	Segurança da Informação
FM	Formulário	**TI**	Tecnologia da Informação
P	Procedimento	**TM**	Termo
PL	Planilha		

3. DESCRIÇÃO DA POLÍTICA

3.1. Políticas de Segurança

Todas as normas devem ser seguidas por todos os funcionários, parceiros e prestadores de serviços. Ao acessar este documento, todos se comprometem a respeitar os tópicos aqui abordados e está ciente de que seus e-mails corporativos e navegação na internet/intranet podem ser monitorados de acordo com a necessidade.

É RESPONSABILIDADE DE TODOS O COMPROMETIMENTO COM OS REQUISITOS DA SEGURANÇA DA INFORMAÇÃO E COM A BUSCA DA MELHORIA DE NOSSO SISTEMA DE GESTÃO.

3.2. Descumprimento das Políticas de Segurança da Informação

O não cumprimento dessas políticas acarreta em sanções administrativas em primeira instância, podendo ocorrer desligamento do funcionário ou rescisão de contrato, de acordo com a gravidade da ocorrência.

3.3. Conscientização de SI

Todos os funcionários devem estar cientes da importância do Sistema de Gestão de Segurança da Informação e dos problemas que podem acarretar quaisquer desvios.

3.4. Gestão da Informação

Toda informação produzida deve ter um proprietário. O proprietário da informação será sempre o gestor a quem a unidade de negócio produtora da informação está subordinada. O proprietário da informação poderá delegar a gestão da informação a um colaborador da unidade de negócio produtora da informação, que administrar á divulgação e a liberação de acessos.

4. DEFINIÇÕES

4.1. Informação

Informação é todo conjunto de dados que tenha sido tratado, agrupado, transformado e/ou consolidado, possuindo valor para a empresa, seu negócio, seus produtos e /ou para seus funcionários, parceiros de negócios, fornecedores e clientes.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

A informação pode se encontrar em várias mídias de transmissão e armazenamento, podendo ser impressa e ou armazenada em meios magnéticos e óticos.

A área competente deverá conhecer o valor de cada informação produzida na Companhia para avaliar a pertinência e a oportunidade de sua liberação para as demais áreas. Toda informação deverá ser classificada como Confidencial, Controlada ou Pública.

Tratamento - As informações devem ser classificadas quanto à confidencialidade, integridade e disponibilidade e identificadas de maneira a serem adequadamente armazenadas e protegidas quanto ao seu acesso e uso. As informações consideradas "segredo do negócio" devem ser destruídas ou deletadas após o descarte. É preciso cuidado na utilização das informações na presença de pessoas não autorizadas ou em locais públicos.

4.1.1. Guarda da Informação

Todos os documentos devem ser armazenados no servidor corporativo, evitando salvar no disco local das estações de trabalho.

Os documentos controlados da SGQSI são acessíveis a todos os funcionários. Devem estar no Diretório Sistema de Gestão da Qualidade e Segurança da Informação sem condições de exclusão, inclusão ou revisão dos documentos.

Os documentos devem ser dispostos quanto à disponibilidade, integridade e confidencialidade aplicáveis.

4.2. Recursos de Tecnologia da Informação

Os recursos de TI abrangem, dentre outros itens:

I - microcomputadores de mesa e portáteis, *tablets*, teclados, mouses, *webcams*, caixas de som, microfones, leitoras de mídia, gravadoras de mídia, *pen drives*, *modems*, dispositivos de armazenamento de certificação digital, placas de *hardware*, *scanners*, impressoras e demais dispositivos periféricos aos computadores;
II - *smartphones*, telefones celulares, telefones de mesa e demais equipamentos relacionados à telefonia da Companhia;
III - programas de computador *(softwares)* adquiridos e sistemas desenvolvidos na Companhia ou por parceiros;
IV - equipamentos e serviços das redes;
V - suprimentos e bens de consumo relacionados à tecnologia da informação;
VI - dados, textos, sons e imagens, sejam estáticas ou dinâmicas, e suas associações, armazenados em equipamentos, dispositivos ou periféricos da Companhia.

4.3. Utilização das informações

As informações são consideradas patrimônio da Comtex. As que forem de caráter crítico e estratégico aos interesses organizacionais devem ser armazenadas nos servidores da rede corporativa, não sendo permitida a gravação de informações particulares nesses servidores.

As informações controladas ou confidenciais não devem ser armazenadas no diretório público.

O funcionário deve comunicar ao Setor de TI pelo Hdesk TI quando detectar a posse ou acesso indevido de qualquer informação, e/ou aplicação indevida de recurso de TI da Companhia.

Os recursos de informação (equipamentos) terão identificação própria de inventário em local visível e não removível a partir do qual será efetuado o controle de entrada e saída ou transferência do respectivo bem patrimonial.

São expressamente proibidas ao funcionário, utilizando equipamentos de TI da Companhia ou em suas dependências as seguintes atividades:

I - Transmissão ou posse de informação que contenha materiais obscenos, indecentes, lascivos ou outro material que explícita ou implicitamente se refira à conduta sexual;
II - Transmissão ou posse de informação que contenha linguagem profana ou constitua apologia ao fanatismo, à prática sexual ou a quaisquer formas de discriminação;
III - Transmissão ou posse de informação que ameace a integridade física ou que intimide outra pessoa ou organização;

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

IV - Transmissão de informação que implique violação de quaisquer leis ou constitua incitamento de qualquer crime;
V - Violação de direitos autorais, particularmente sobre software, dados e publicações;
VI - Divulgação de qualquer informação restrita ou confidencial sem a permissão de seu proprietário ou do Gestor do recurso ao qual a informação pertence.

4.4. Transferência das informações

A transferência de informação é o momento mais delicado e de vulnerabilidade da informação. Carece, portanto, de cuidado. Antes de transferir qualquer informação, por e-mail, whatsApp, telefone, ou outro meio de comunicação, verifique se você tem autorização para passá-la, se a pessoa a receber tem condições de recebê-la e qual a consequência de tal transferência.

4.4.1. Documentos Impressos

Não deixe material impresso nas impressoras. Retire o que for impresso, sempre.

Fragmente todo material confidencial que foi impresso. Caso tenha dúvida quanto à confidencialidade do documento, **FRAGMENTE-O**.

NUNCA JOGUE EM LATAS DE LIXO MATERIAL CONFIDENCIAL OU CONTROLADO.

5. FUNÇÕES E RESPONSABILIDADES

5.1. Administradores e Funcionários

Ficam responsáveis por alcançar os objetivos, manter o controle sobre a segurança das informações armazenadas nos equipamentos que estão sob sua responsabilidade, e:

- Remover dos servidores as informações que estejam desatualizadas, que não sejam mais necessárias ao desempenho do trabalho, ou que se refiram a assuntos alheios aos interesses da Companhia;

- Atos e acessos realizados com sua identificação no ambiente informatizado;

- Manter o sigilo sobre as informações consideradas estratégicas e confidenciais da Companhia;

É proibida a criação, a modificação, a execução ou a retransmissão de quaisquer instruções ou programas de computador com o intuito de obter acesso não autorizado a um recurso, equivalendo, no caso, tentativa de "quebra" da segurança de sistemas.

5.2. Gestor de Área

Cada Gestor de Área é responsável pela disponibilização do acesso às informações sob sua administração.

Responsabilidades:

- Informar o Setor de TI das respectivas necessidades de acesso aos recursos pelos funcionários ou contratados;
- Classificar segurança das informações e dos recursos sob sua responsabilidade, bem como validar, liberar e cancelar o acesso dos funcionários às informações e aos recursos da sua área quando necessário;
- Supervisionar adequadamente os recursos sob sua responsabilidade, de forma a preservar sua integridade física e bom funcionamento.

5.3. Parceiros e Terceiros

Acordos de confidencialidades e de acesso às informações contidas nesta política devem existir contratualmente para observância e cumprimento.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

5.4. Setor de TI

5.4.1. Atribuições da Área de TI

É atribuição do Setor de TI prover os instrumentos tecnológicos necessários ao cumprimento das normas estabelecidas nesta Política, bem como zelar pela manutenção, devidamente atualizada, de sistemas operacionais, navegadores e quaisquer programas de detecção e eliminação de códigos e/ou programas indevidos nas estações de trabalho dos usuários. Os recursos de informática, os endereços da Internet visitados e as mensagens que trafegam no serviço de correio eletrônico ou em qualquer outro serviço da rede serão monitorados com vistas à prevenção e fiscalização do uso indevido desses recursos.

O Setor de TI por medida de segurança poderá bloquear temporariamente, sem aviso prévio, o acesso a recurso de tecnologia da informação de qualquer funcionário que esteja realizando atividade que coloque em risco a segurança da rede ou que represente uso indevido de tal recurso.

Realizado o bloqueio mencionado, a área de TI comunicará imediatamente o ocorrido ao usuário responsável e ao seu Gestor.

O desbloqueio do recurso de tecnologia da informação só ocorrerá após anuência por escrito do Gestor, e desde que não represente risco de dano à infraestrutura tecnológica da Companhia.

5.4.2. Administração dos recursos de Tecnologia da Informação

Os administradores dos sistemas computacionais da Comtex são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Entende-se por administradores de sistemas computacionais quaisquer pessoas integrantes da área de TI, do quadro funcional ou não, que tenham conhecimento autorizado do código de acesso e senha de administração dos recursos de tecnologia da informação, sejam eles de uso geral ou de uso restrito a uma unidade, grupo de pessoas ou de uso individual.

5.4.3. Serviços de Suporte ao Usuário

Todas as solicitações de suporte ao usuário devem ser efetuadas mediante ferramenta de gestão de chamados da Companhia (Hdesk TI). É proibido o uso do serviço de suporte ao usuário em caráter particular, sem aplicação objetiva na atividade institucional, ou ainda quando relacionado a produtos ou tecnologias não homologadas pela área de TI.

6. SEGREGAÇÃO DE FUNÇÃO

Com o objetivo de reduzir as oportunidades de modificação, não autorizada ou não intencional, ou uso indevido dos ativos da organização, as funções da Comtex devem ser segregadas com base na metodologia RACI, que identifica o Responsável por executar a atividade. O dono da atividade é chamado de Autoridade. Será atribuída apenas uma autoridade por atividade. Consultado é aquele que deve ser consultado a participar da decisão ou atividade no momento em que for executada. O Informado deve receber a informação de que uma atividade foi executada e quem a executou.

Cabe a todos os funcionários, terceiros e prestadores de serviço seguir as regras definidas de responsabilidades na Planilha de Segregação de Função divulgada. Em caso de dúvida, deve ser procurado o gestor da área.

7. COMUNICAÇÃO

Todas as informações divulgadas nos quadros de avisos, Facebook e Linkedin devem ser exclusivamente públicas e de responsabilidade da área de Comunicação.

As ferramentas que tenham a finalidade de estabelecer a comunicação interna e externa devem ser mapeadas e classificadas em: o que comunicar, quando comunicar, classificação da informação, quem será o comunicado e o processo pelo qual a comunicação será realizada.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

8. RISCOS

Todos os funcionários devem conhecer os riscos de segurança da informação de seus processos e zelar para que não ocorram danos que possam ter impactos ao SGSI e ao nosso maior bem: A INFORMAÇÃO.

Os riscos identificados na Companhia deverão ser monitorados e tratados. Riscos que serão aceitos deverão atender a critérios predefinidos.

9. REQUISITOS LEGAIS

É dever dos funcionários buscar conhecer e cumprir os requisitos legais aplicáveis. A Comtex é uma empresa idônea e como tal zela e preza pelo seu bom direcionamento e gerenciamento estratégico. Um desses gerenciamentos é atender a tais requisitos e fazer cumpri-los. Portanto, se chegar a você um comunicado de atendimento a uma regra legal, cumpra-a.

10. MESA LIMPA E TELA LIMPA

Informações confidenciais e controladas, independente do formato, não devem ficar expostas nas mesas e impressoras, arquivadas em armários e gavetas destrancadas, disponíveis em quadros e telas de computadores de forma imprudente.

É proibido ter arquivos salvos nas áreas de trabalho.

11. DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

11.1. Atendimento ao Cliente (Consignado)

Não é permitido o trabalho remoto ou acessos por dispositivos não autorizados ao sistema de atendimento ao cliente do consignado, os bloqueios dos acessos devem ser por endereço IP.

11.2. Outras áreas

O trabalho remoto deve ser autorizado por gestores e realizado através de VPN, mediante solicitação formal ao setor de TI.

O e-mail corporativo é a única ferramenta que pode ser utilizada em dispositivo móvel não homologado na área de TI, devendo os cuidados serem o mesmo dos itens 4.3 e 4.4.

11.3. Dispositivos móveis

Não é permitido o uso de dispositivos móveis em equipamentos corporativos. Quando houver necessidade de transferência de arquivo, deve ser solicitado um chamado no Hdesk para a área de TI, que avaliará e realizará a transferência em equipamento específico.

12. BACKUP

O Setor de TI deverá executar cópias de segurança dos servidores corporativos, devendo o funcionário comunicar, via ferramenta de gestão de chamados, a necessidade de recuperação de arquivos neles armazenados em caso de falha. Este comunicado deve contemplar a caracterização de confidencialidade da informação e tempo máximo para a disponibilização da mesma.

O Setor de TI proporcionará tecnologias em que o backup das informações ocorrerá de forma automatizada. Contudo, para que o backup seja realizado, caberá ao funcionário manter os dados e informações nos servidores corporativos, visando o compartilhamento de acordo com a confidencialidade.

O funcionário solicitará a restauração da cópia de segurança ao Setor de TI que, após análise, verificando o propósito e nível de acesso à informação, autorizará ou não a restauração da mesma.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

13. ACESSOS

13.1. Permissões de acesso a terceiros

A conexão de equipamentos de terceiros ou de propriedade particular do funcionário na rede interna é proibida. A execução de trabalhos de terceiros contratados só deverá ser feita com a prévia autorização do Setor de TI.

Para visitantes e outros usuários que não sejam funcionários, a permissão de acesso à rede deve ser autorizada por um patrocinador e o Setor de TI, que seguirá os procedimentos existentes para a atribuição de permissões de acesso, bem como para revogá-las e monitorá-las. O patrocinador será responsável pelas ações do usuário e, portanto, deverá monitorá-lo.

As permissões de acesso para visitantes devem ser válidas somente durante a permanência do mesmo na Companhia.

A violação desta política pode causar a suspensão temporária ou definitiva do seu acesso à rede corporativa, além de sujeitar o infrator às consequências previstas em lei. No caso de prestadores de serviços, o contrato de prestação de serviços será passível de cancelamento, além de outras penalidades legalmente cabíveis.

Os acessos à rede Comtex por visitantes serão realizados em rede segregada.

13.2. Controle de acesso a recursos de funcionários

Os funcionários devem ter acesso liberado somente aos recursos necessários ao desempenho de suas atividades e em conformidade com os interesses institucionais. A comunicação da necessidade de acesso a um recurso deve ser feita por um Gestor de área, através de chamado.

Compete ao Gestor controlar a identificação dos funcionários sob sua supervisão e informar o RH sobre os casos de desligamento, afastamento ou transferência.

O fluxo de informações para o ambiente externo deve passar através de um ponto de controle de forma a garantir que sejam liberadas apenas informações autorizadas.

13.3. Desligamento de funcionário (acesso)

O demandante deverá entregar o formulário de Requisição de Desligamento devidamente assinado no RH, inclusive nos casos em que o funcionário tenha solicitado o desligamento, visando assegurar a condução do processo de maneira segura para os interesses da Companhia.

Após conclusão do processo de desligamento do funcionário, a área de RH deverá enviar um comunicado para as áreas: Administrativa, para bloqueio dos acessos físicos; TI, para bloqueio de acessos lógicos; e Gestão de pessoal, para providências contratuais.

13.4. Aplicação a Terceiros

Os contratos de prestação de serviços celebrados com a Comtex em que haja a eventual ou efetiva utilização de recursos de informática da Companhia devem cumprir esta Política pelos prepostos por ela alocados, bem como podem ocorrer penalidades decorrentes da sua inobservância.

13.5. Compartilhamento de informações

O compartilhamento de informações em arquivos pela estrutura do Google Drive, que inclui formulários, planilhas, apresentações e documentos diversos, somente é permitido para usuários que estão dentro do domínio da Companhia, sendo o seu compartilhamento com usuários externos desautorizado.

13.6. Acesso físico às instalações

Os acessos às áreas devem ser realizados pelo EyeLock, com prévio cadastramento da íris.

O uso do crachá é obrigatório para todos os funcionários, terceiros e visitantes no interior da Comtex. Caso algum usuário tenha o seu crachá extraviado, deverá solicitar um novo na recepção de sua unidade. Visitantes devem devolver o crachá ao sair.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©

Todo funcionário só terá acesso às áreas que forem de interesse de sua atividade. Acessos eventuais só poderão ocorrer com autorização do gestor da área de interesse.

Os acessos de visitantes no interior da Comtex só poderão ocorrer com autorização de cargos de Gestão. Nenhum visitante está autorizado a entrar sem o cadastro na recepção.

Atividades realizadas por terceiros deverão ser acompanhadas pelo solicitante, sendo considerado inadmissível o trânsito de terceiros desacompanhados.

Parceiros poderão transitar pela unidade desacompanhados somente nas áreas que forem necessárias para execução de suas atividades com cadastro no EyeLock, com tempo de término para bloqueio definido pelo cargo de gestão que autorizou o acesso.

Atividades de recrutamento e seleção, desligamentos, atendimentos a ex-funcionários e atividades que não necessitem da entrada em ambientes Comtex deverão ocorrer na sala externa próxima à recepção.

Todos os funcionários desligados deverão ter seu acesso cancelado no EyeLock mediante comunicação do RH.

13.7. Compartilhamento de credencial de acesso

Jamais poderão ser compartilhadas informações de credenciais de acesso lógico.

Ao acionar uma porta com a sua íris, um funcionário pode autorizar que outro também use este acesso na mesma passagem nos ambientes comuns, sendo esta ação, contudo, proibida para estranhos. Para os ambientes não comuns e com controle de acesso (Diretoria, CPD Uruguaiana, TI, S4C, Gestão de Pessoal e acesso externo da entrada de serviços do 22º), um funcionário que não possua acesso não pode se beneficiar da íris de terceiros autorizados, exceto em casos em que exista autorização do gestor da área.

É vedada a permanência de pessoas não autorizadas na linha de atendimento do Consignado.

13.8. Cadastramento de Usuários

As concessões e retiradas de acessos serão realizadas mediante comunicação da área de RH, de Administração de Pessoal ou do Gestor do terceiro que está iniciando o seu contrato ou suas atividades, tendo as contas de acesso dos funcionários e contratados prazo de validade de acordo com a vigência do contrato de trabalho com a Companhia ou do projeto em execução.

Nos casos em que o cadastramento não ocorra automaticamente em novos contratos, caberá ao Gestor solicitá-lo via ferramenta de gestão de chamados ao Setor de TI, formalizando necessidades de acesso e uso de recursos pelo novo funcionário ou contratado.

Quando houver a saída do funcionário da Companhia, caberá à Administração de Pessoal ou ao Gestor Imediato informar ao Setor de TI, via ferramenta de gestão de chamados, para que seja feita a exclusão do usuário.

Nas alterações de cargo, transferências setoriais ou de unidade, o superior imediato deve solicitar a revogação das antigas permissões através de abertura de chamado.

14. OBJETIVOS E ANÁLISE DA POLÍTICA

Os objetivos do SGSI estão descritos no (MSI-001) Manual Estratégico de SGSI, assim como a periodicidade da análise crítica e as questões internas e externas que devem ser levadas em consideração.

Este documento é de propriedade da Comtex. Todos os direitos reservados. ©