



## **Política de Segurança**





## Índice

---

Introdução .....	3
Objetivo.....	4
Responsabilidades.....	5
Área de Tecnologia da Informação .....	6
Segurança da Informação.....	8
Mecanismos de Segurança .....	9
Ameaças à Segurança.....	10
Monitoramento do Ambiente .....	11
Computadores e Recursos Tecnológicos .....	12
Dispositivos Móveis .....	14
Datacenter .....	16
Uso do Correio Eletrônico .....	17
Acesso a Internet.....	19
Download de Arquivos .....	20
Usuário e Senha .....	21
Comunicação Via Internet.....	23
Checagens/Atualizações .....	24
TI - Contatos .....	25
Glossário.....	27
Bibliografia .....	28
Anexos .....	29

---



## Introdução

A política de segurança é um conjunto formal de regras a serem seguidas pelos utilizadores dos recursos de uma organização (colaborador e prestadores de serviço), para a proteção dos ativos de informação e a prevenção de responsabilidade para todos os usuários. Devem, portanto, ser cumpridas e aplicadas em todas as áreas da organização, levando em consideração duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não proibido é permitido).

*Entenda-se “organização” ou “instituição” todas as empresas do grupo, que são:*

- *CGSC Holding Brasil*
- *Cooper Gay do Brasil*
- *Swett Crawford Brasil*



## **Objetivo**

Definir normas e procedimentos específicos relacionados à segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Os objetivos deste guia são:

- garantir a segurança e acesso à informação
- organizar e controlar o uso de equipamentos e software
- formalizar as ações e procedimentos



## Responsabilidades

- 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 um termo de responsabilidade (*conforme Anexo I*).
- É obrigação de cada colaborador manter-se atualizado em relação a este guia e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Área de TI sempre que ele não estiver absolutamente seguro quanto ao uso da informação e/ou de ativos e/ou sistemas de informação.
- Todo incidente que afete a segurança da informação deverá ser comunicado à Área de TI.
- 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 de acesso à informação.
- A política de segurança deve ser implementada por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.
- O não cumprimento das Normas de Segurança da Informação acarretará violação às regras internas da instituição.



## Área de Tecnologia da Informação

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

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências (log) que permitam a rastreabilidade para fins de auditoria ou investigação.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a organização.

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

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

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

*Os 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 a execução de atividades operacionais sob sua responsabilidade.*



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

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da organização;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da organização;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

A formalização de ações e processos relacionados a TI deve ser seguida de modo a padronizar e documentar solicitações de:

- Aquisição (hardware, software, periféricos, serviços, etc...);
- Desenvolvimento (projeto, sistema, programas, etc...);
- Manutenção (programas, hardwares, periféricos, etc...).

A solicitação deve ser enviada por e-mail para a Área de TI e esta deve registrar em documento padrão da área, a Ordem de Serviço (*conforme Anexo II*).



## Segurança da Informação

Informações podem ser dados, conteúdos ou documentos que tenham valor para um indivíduo ou para a organização.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada, pertence à referida instituição.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A instituição, por meio da Área de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Cabe a Área de TI montar um Plano de Continuidade de Negócio, visando assegurar a continuidade do negócio durante e após qualquer incidente crítico que resulta em interrupção de sua capacidade operacional normal.

- Garantir a cópia de segurança (backup) de arquivos e dados;
- Garantir o acesso dos colaboradores a este backup, se necessário.

*A restauração de um backup (completa ou parcial) deve ser solicitada à Área de TI por meio formal (e-mail) e após a conclusão da tarefa, a mesma deve ser registrada formalmente pela Área de TI na Ordem de Serviço.*

As informações devem ser armazenadas preferencialmente eletronicamente, caso tenham sido impressas, devem ser digitalizadas e armazenadas no drive de rede, nas pastas específicas.

As informações devem ser mantidas por tempo determinado de acordo com a legislação pertinente e requisitos de negócio. Devem-se manter trilhas das informações, mantendo-se estados e situações quando for necessária alguma comprovação de que as informações existiram e foram processadas com determinadas características.

**Os recursos de informação (documentos, equipamentos, mídias...), quando forem descartados, devem ser tratados de maneira a não permitir a recuperação das informações por terceiros.**





## Mecanismos de Segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- **Controles físicos:** são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controles físicos:

Portas / trancas / paredes / blindagem / guardas / etc ..

- **Controles lógicos:** são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Senhas / sistemas biométricos / firewalls / cartões inteligentes / anti-vírus / etc...



## Ameaças à Segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

- **Perda de Confidencialidade:** seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- **Perda de Integridade:** aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
- **Perda de Disponibilidade:** acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

*No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como hackers. Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro.*



## **Monitoramento do Ambiente**

- Se necessário, implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de solicitação do gerente (ou superior);
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade (ex.: atualização de softwares, limpeza de disco, etc...);
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações (ex.: anti-vírus).



## Computadores e Recursos Tecnológicos

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

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Área de TI. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Área de TI, ficando responsáveis pelas ações realizadas.

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 a Área de TI para obter as instruções devidas.

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

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

Cada colaborador tem acesso somente à pasta de rede relacionada à sua área de trabalho. O acesso às demais pastas (de outras áreas) será fornecido pela Área de TI mediante solicitação formal do gestor da área solicitante.

A pasta de rede TEMP deve ser utilizada para armazenar arquivos temporários (troca entre áreas, downloads, etc...), portanto, para garantir disponibilidade de espaço físico no drive de rede, a mesma será apagada sempre na noite do último dia de cada mês.



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

- Todos os computadores de uso individual deverão ter senha para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Área de TI.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- 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 designado pela Gerência de Sistemas.
- Os modems internos ou externos podem ser utilizados alguns casos de deslocamentos ou para planos de contingência.
- Deve ser evitado ao máximo o consumo de alimentos e bebidas na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela organização, seguindo os devidos controles de segurança exigidos pela Política de Segurança e pelas normas específicas da instituição.
- Todos os recursos tecnológicos adquiridos pela organização devem ter imediatamente suas senhas padrões (default) alteradas.

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

- 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.
- Interromper um serviço, 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 propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.



## Dispositivos Móveis

A organização deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Área de TI, como: notebooks, smartphones, tablets e pendrives.

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.

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

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel (se for o caso). Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.


Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel (se possível).

O suporte técnico aos dispositivos móveis de propriedade da organização e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

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 Área de TI.

Deve-se buscar orientação junto a Área de TI quando forem executadas atualizações de versões do sistema operacional.

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 Área de TI.



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.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela organização notificar imediatamente seu gestor direto e a Área de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

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 organização e/ou a terceiros.

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

Equipamentos portáteis, como smartphones, tablets, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, poderão não ser validados e autorizados para uso e conexão com a rede corporativa e com a rede sem fio da organização.



## **Datacenter**

O Datacenter deve manter-se fechado por meio de chave, com ambiente apropriado para o funcionamento (ex.: ar condicionado em constante funcionamento, extintor de incêndio acessível, etc...).

O acesso ao Datacenter somente deverá ser feito por pessoas previamente autorizadas, visando a não interrupção dos serviços:

- Servidor de arquivos
- Acesso à rede interna
- Acesso à internet
- Telefonia

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

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

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

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a liberação dos colaboradores previamente autorizados.





## Uso do Correio Eletrônico

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

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

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a organização vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a organização estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
  - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da organização;
  - Contenha ameaças eletrônicas, como: spam, vírus de computador;
  - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - Vise obter acesso não autorizado a outro computador, servidor ou rede;
  - Vise burlar qualquer sistema de segurança;
  - Vise acessar informações confidenciais sem explícita autorização do proprietário;
  - Contenha anexo(s) superior(es) a 10 MB para envio (interno e internet) e 10 MB para recebimento (internet)
  - Tenha conteúdo considerado impróprio, obsceno ou ilegal;



- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
- As mensagens de correio eletrônico sempre deverão incluir assinatura com os dados do colaborador e da empresa do grupo (conforme Anexo III).

*O uso da rede sem fio (Wi-Fi), também é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a organização e também não cause impacto no tráfego da rede sem fio.*

*Para utilizar a rede sem fio o colaborador, visitante ou prestador de serviço deverá solicitar a senha de acesso à Área de TI, que será responsável por documentar a solicitação.*

*Periodicamente a Área de TI deve alterar a senha de acesso à rede sem fim para evitar que autorizações de acesso antigas fiquem ativas indefinidamente. A periodicidade máxima para troca da senha é 90 (cento e oitenta) dias.*

***Dica:*** *Desconfie de e-mails de fontes desconhecidas ou inesperadas, normalmente são e-mails falsos enviados com a intenção de prejudicar ou obter algum tipo de vantagem do destinatário (ex.: dados pessoais ou bancários). Ao receber um e-mail suspeito contate imediatamente a Área de TI informando o fato para receber as devidas instruções. Em hipótese alguma abra o e-mail, mas caso tenha acontecido, não clique em links ou imagens ou execute o download de arquivos.*



## **Acesso a Internet**

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

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

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

A organização, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades. Como é do interesse da organização 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.



## Download de Arquivos

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades da organização e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Área de TI.

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 Área de TI.

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

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias.

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

O acesso a softwares peer-to-peer (eMule, Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisiite formalmente à Gerencia de Sistemas.



## Usuário e Senha

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

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login e/ou senha de uso compartilhado por mais de um colaborador, a responsabilidade perante a organização será dos usuários que dele se utilizarem. É proibido o compartilhamento de login e/ou senha para funções de administração de sistemas.

A Área de TI responde pela criação da identidade lógica dos colaboradores na instituição (sistemas, rede de computadores).

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

A identificação (login) irá seguir a regra de formação do e-mail do colaborador, composta por *Nome, ponto, Sobrenome* (ex.: Marcos Aurélio Cunha => e-mail: [marcos.cunha@organização.com.br](mailto:marcos.cunha@organização.com.br) => login: [marcos.cunha](#))


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

As senhas não devem ser 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.

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

A periodicidade máxima para troca das senhas é 180 (cento e oitenta) dias.

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 ao Departamento de Tecnologia da Informação, a fim de



que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado.

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

Cada conta de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação pertence exclusivamente a um responsável identificável como pessoa física, sendo que:

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



## Comunicação Via Internet

A Área de TI disponibilizará ferramentas de comunicação de voz e vídeo (interna/externa) via internet visando facilitar a comunicação entre os colaboradores da organização e reduzindo o custo desta comunicação. São elas:

- Skype
  - Permitem comunicação para telefones fixos e celulares, no Brasil e no exterior.
  - De Skype para Skype não há custo na ligação, porém para telefones fixos e celulares há a necessidade do pagamento de “créditos” para utilização do mesmo.
- Lync
  - Permite a comunicação entre grupos e/ou indivíduos da organização que estejam no mesma estrutura de serviço do Microsoft Office 365 (ferramenta corporativa para colaboração e compartilhamento).

Responsabilidades:

- Área de TI
  - Criar e divulgar um Manual de Utilização das Ferramentas de Comunicação Via Internet.
  - Instalar, configurar e treinar os colaboradores quanto ao uso das Ferramentas de Comunicação Via Internet.
- Colaboradores
  - Utilizar as Ferramentas de Comunicação Via Internet visando padronizar a comunicação entre colaboradores e/ou grupos de colaboradores da organização e ainda, a redução de custos da comunicação.



## Checagens/Atualizações

A Área de TI realizará checagens e atualizações periódicas dos Sistemas de Informações, Computadores e Recursos Tecnológicos, visando garantir a conformidade e constante melhoria da Política de Segurança da organização.

Referência	Tipo	Periodicidade
Internet	Checagem de disponibilidade e desempenho	Mensal
Microsoft Office 365	Checagem de disponibilidade e desempenho	Mensal
Rede sem fio	Checagem de disponibilidade e desempenho	Mensal
Firewall	Checagem de disponibilidade e desempenho	Mensal
Sistemas de Informações	Checagem de disponibilidade e desempenho	Mensal
Sistemas de Informações	Checagem de log de acesso	Mensal
Skype	Checagem de disponibilidade e desempenho	Mensal
Skype	Checagem de uso	Mensal
Manutenção dos computadores	Prevenção de disponibilidade e desempenho	Semestral
Manutenção de impressoras	Prevenção de disponibilidade e desempenho	Semestral
Troca de senha MS Office 365	Controle de acesso	Semestral
Troca de senha Sistemas de Informações	Controle de acesso	Semestral
Troca de senha Rede sem fio	Controle de acesso	Semestral
Teste do Plano de Continuidade de Negócio	Prevenção de disponibilidade e desempenho	Anual





## TI - Contatos

### Equipe:

Name	Phone	E-mail
<i>Jorge Almeida</i> <i>IT Manager</i>	Direct Number (55 21) 2272-5225 Mobile Number (55 21) 8122-5006 Home Number (55 21) 2254-4669	<i>jorge.almeida@cogbrasil.com.br</i>
<i>Responsibilities:</i> <ul style="list-style-type: none"><li><i>Project Management</i></li></ul>		

Name	Phone	E-mail
<i>Marcus Vinicius</i> <i>Analyst Programmer</i>	Direct Number (55 21) 2272-5235 Mobile Number (55 21) 9185-7321 Home Number (55 21) 2288-9840	<i>marcus.vinicius@cogbrasil.com.br</i>
<i>Responsibilities:</i> <ul style="list-style-type: none"><li><i>System development</i></li></ul>		

Name	Phone	E-mail
<i>Thiago Araujo</i> <i>Analyst Support</i>	Direct Number (55 21) 2272-5229 Mobile Number (55 21) 8237-9796 Home Number (55 21) 3662-2105	<i>thiago.araujo@cogbrasil.com.br</i>
<i>Responsibilities:</i> <ul style="list-style-type: none"><li><i>Helpdesk</i></li></ul>		

### Área de TI – Grupo de E-mail:

E-mail
<i>ti.division@cogbrasil.com.br</i>

### Terceirizados:



Name	Phone	E-mail
<i>João Carlos</i> <i>Tech Desk - RJ</i>	Direct Number (55 21) 2210-1756 Mobile Number (55 21) 8100-1755	<i>jmendes@techdesk.com.br</i>
<i>Responsibilities:</i> <ul style="list-style-type: none"><li>• <i>Project Management</i></li></ul>		

Name	Phone	E-mail
<i>Alex</i> <i>Tech Desk - SP</i>	Direct Number (55 11) 9456-7718 Mobile Number (55 11) 8084-7718	<i>infolyde@gmail.com</i>
<i>Responsibilities:</i> <ul style="list-style-type: none"><li>• <i>Helpdesk</i></li></ul>		



## Glossário

Hardware	<ul style="list-style-type: none"><li>• Parte física, o computador e dispositivos de entrada e saída.</li></ul>
Software	<ul style="list-style-type: none"><li>• Parte lógica, o conjunto de instruções e dados processado pelos circuitos eletrônicos do <i>hardware</i>.</li></ul>
Download	<ul style="list-style-type: none"><li>• Transferência de dados de um computador remoto para um computador local.</li></ul>
Backup	<ul style="list-style-type: none"><li>• Cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais.</li></ul>
Firewall	<ul style="list-style-type: none"><li>• Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança de acesso externo a esta rede de computadores.</li></ul>
Log	<ul style="list-style-type: none"><li>• Processo de registro de eventos relevantes num sistema computacional.</li></ul>
Vírus	<ul style="list-style-type: none"><li>• Software malicioso que vem sendo desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.</li></ul>
Trojans	<ul style="list-style-type: none"><li>• Programa malicioso que age como a lenda do cavalo de Troia, entrando no computador e liberando uma porta para uma possível invasão de outro computador.</li></ul>
Periféricos	<ul style="list-style-type: none"><li>• Qualquer equipamento acessório que seja ligado ao computador.</li></ul>
Wi-Fi	<ul style="list-style-type: none"><li>• Acesso à Internet sem o uso de cabos.</li></ul>
Drive	<ul style="list-style-type: none"><li>• Refere-se à unidade de armazenamento ou de leitura de dados.</li></ul>
Datacenter	<ul style="list-style-type: none"><li>• É o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização.</li></ul>
Spam	<ul style="list-style-type: none"><li>• Consiste numa mensagem de correio eletrônico não-solicitada, enviada com fins publicitários.</li></ul>
Peer-to-peer	<ul style="list-style-type: none"><li>• Compartilhamento de dados e recursos numa larga escala eliminando qualquer requisito de servidores.</li></ul>
Login	<ul style="list-style-type: none"><li>• Identificação para acesso a um sistema.</li></ul>



## Bibliografia

John TERPSTRA. *Segurança para Linux*. RJ: Elsevier, 2005. [ISBN 85-352-1599-9](#)

SENAC São Paulo, Gerência de Sistemas – Segurança da Informação.



## Anexo II



### Política de Segurança

#### Endosso do Empregado

Endossar esta política equivale a declarar seu compromisso pessoal com a integridade da informação e recursos tecnológicos da Cooper Gay do Brasil.

Por favor, leia o *Manual da Política de Segurança* com cuidado. Depois que tiver terminado, responda às seguintes questões, assine, date e devolva este formulário a Recursos Humanos.

**Nome do Funcionário**

**Cargo**

**Data de Admissão**

**Matrícula**

**Área**

**Sucursal**

	<b>SIM</b>	<b>NÃO</b>
1. Você recebeu e leu o <i>Manual da Política de Segurança</i> da Cooper Gay do Brasil?	<input type="checkbox"/>	<input type="checkbox"/>
2. Você tem ou pensa que pode ter quaisquer conflitos de interesse a relatar? (Se responder "Sim", será enviado a você um formulário de Conflito de Interesses para ser preenchido e devolvido ao Recursos Humanos)	<input type="checkbox"/>	<input type="checkbox"/>
3. Você compreende suas responsabilidades tal como esquematizadas neste Manual, e concorda em praticá-las?	<input type="checkbox"/>	<input type="checkbox"/>

\_\_\_\_\_  
(assinatura)

\_\_\_\_\_  
(data)

Política de Segurança – CGSC

### Anexo III

<b>Jorge Ricardo Neves de Almeida</b> IT & Compliance	
	
<b>CGSC Holding Brasil Ltda</b> Av. Presidente Wilson, 165/1115, Rio de Janeiro/RJ - CEP 20.030-020 Tel: +55 (21) 2272 5225   Fax: +55 (21) 2272 5220   Mob: +55 (21) 8122 5006 Email: <a href="mailto:jorge.almeida@cogbrasil.com.br">jorge.almeida@cogbrasil.com.br</a> Website: <a href="http://www.cg-sc.com">www.cg-sc.com</a>	
Jorge Ricardo Neves de Almeida	Nome do colaborador
IT & Compliance	Cargo ou área
CGSC Holding Brasil Ltda Av. Presidente Wilson, 165/1115, Rio de Janeiro/RJ - CEP 20.030-020	Dados da empresa
Tel: +55 (21) 2272 5225   Fax: +55 (21) 2272 5220   Mob: +55 (21) 8122 5006	Telefones de contato
Email: <a href="mailto:jorge.almeida@cogbrasil.com.br">jorge.almeida@cogbrasil.com.br</a>	Endereço de e-mail