POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de segurança da informação, na GCS, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à GCS. Todo e qualquer usuário de recursos computadorizados da Companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

1. Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
2. Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
3. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da GCS. Este documento deve ser levado a conhecimento dos membros do grupo de confidencialidade e imparcialidade.

MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da GCS. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

É DEVER DE TODOS Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a GCS e deve sempre ser tratada profissionalmente.

CLASSIFICAÇÃO DA INFORMAÇÃO É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

Pública	Interna	Confidencial	Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

DADOS DOS FUNICIONÁRIOS

A GCS se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários que porventura sejam armazenados, serão considerados dados confidenciais. Dados Pessoais de Funcionários sob a responsabilidade da GCS não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (*e-mails*) usados pelos funcionários da GCS. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da GCS, sem prévia e expressa autorização por parte da diretoria. Mesmo que seja autorizado o armazenamento destes dados, a GCS não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores de empresa, e jamais poderão fazer parte da rotina de *backup* da GCS.

ADMISSÃO E DEMISSÃO DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da Companhia deverá informar ao setor de TI, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Companhia. Isto inclui o fornecimento de sua senha ("*password*") e registro do seu nome como usuário no *sistem*, pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de TI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o setor de Recursos

Humanos deverá comunicar o fato o mais rapidamente possível ao departamento de TI, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da GCS. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

TRANSFERÊNCIA DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de TI, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

PROGRAMAS ILEGAIS

A GCS respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da GCS. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na GCS.

Os usuários não podem, em hipótese alguma, instalar este tipo de "*software*" (programa) nos equipamentos da Companhia, mesmo porque somente o pessoal da área de Ti tem autorização para instalação de programas previamente autorizados dentro da política de segurança da companhia. Periodicamente, o Setor de Informática fará verificações nos dados dos servidores ou nuvem e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores. Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos os sansões previstas neste documento. Recomendamos estas mesmas práticas para os nossos parceiros de negócios e prestadores de serviços terceirizados.

PERMISSÕES E SENHAS

Todo usuário para acessar os dados da rede da GCS, devera possuir um *login* e senha previamente cadastrados pelo pessoal de TI. Quem deve fornecer os dados referente aos direitos do usuário é o responsável direto pela sua chefia, que deve preencher uma ficha e entregá-la ao departamento de RH. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, por meio de memorando ou *e-mail*, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro *login* e após isso a cada 90 (noventa) dias. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc) deverão comunicar ao Setor de TI qual será o seu substituto quando de sua ausência da GCS, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de TI. Alguns documentos são de uso restrito ou estarão disponíveis apenas para consulta.

COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de pastas nos computadores e *desktops* da GCS, salvo se autorizado. Todos os dados deverão ser armazenados nas redes apropriadas da rede, e a autorização para acessá-los deverá ser fornecida pelo TI. O Pessoal de TI está orientado a periodicamente todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede. Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso. Não

são permitidos na GCS o compartilhamento de dispositivos móveis tais como pen-drivers e outros, salvo se autorizado pela área de TI ou Alta Direção.

BACKUP (COPIA DE SEGURANÇA DOS DADOS)

Todos os dados da GCS são protegidos através de rotinas sistemáticas de *Backup*. Os *Backups* são realizados diariamente a partir das 00h de *Salt Lake City*, e a cada conclusão da semana, as 00h de segunda, os *Backups* são compilados em *Backups* semanais e as cópias de segurança do sistema integrado são de responsabilidade do Setor de TI da matriz, encaminhando semanalmente o código de rastreabilidade do *Backups*. Se necessário, os *Backups* pode ser resgatado em um padrão normal de 72h ou em situações emergenciais em até 4 horas. A GCS Brasil possui o suporte da DW Malagodi IT, que é par da área de TI de *Salt Lake City*.

Alguns documentos poderão ser protegidos por senha e o controle dica com a Alta Direção e área de TI.

Como segunda ferramenta de gestão da segurança da informação, semanalmente, as sexta-feira, o Diretor Operacional, realiza um *backup* em rede nuvem segura e isolada das redes GCS Brasil. A GCS não faz *backup* armazenado externamente em mecanismos móveis.

CÓPIAS DE SEGURANÇA DE ARQUIVOS EM *DESKTOPS*

Não é política da GCS o armazenamento de dados em *desktops* individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede. Nestes e em outros casos, o pessoal de TI deverá alertar ao usuário que ele deve fazer *backup* dos dados de sua máquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("*backups*") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da GCS. No caso das informações consideradas de fundamental importância para a continuidade dos negócios da GCS o Setor de Informática disponibilizará

um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de *backup* da Informática.

SEGURANÇA E INTEGRIDADE DOS DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Ti, assim como a manutenção, alteração e atualização de equipamentos e programas.

PROPRIEDADE INTELECTUAL

É de propriedade da GCS, todos os "*designs*", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a GCS.

PROPRIEDADE INTELECTUAL

O acesso à *Internet* é autorizado, inclusive para rápida navegação de assuntos particulares, entretanto, sites que podem trazer segurança ao sistema de TI, ou sites com conteúdo inapropriados e não condizentes com a política e princípios éticos e de compliance da GCS, é proibido. O uso da *Internet* será monitorado pelo Setor de Informática, inclusive através de "*logs*" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a *Internet* e qual página acessou.

Não é permitido instalar programas provenientes da *Internet* nos microcomputadores da GCS, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na *Internet*, é proibido a visualização, transferência (*downloads*), cópia ou qualquer outro tipo de acesso a sites:

a) De conteúdo pornográfico ou relacionados a sexo;
b) Que defendam atividades ilegais;
c) Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
d) Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da GCS;

e) Que promovam discussão pública sobre os negócios da GCS, a menos que autorizado pela Diretoria;

f) Que possibilitem a distribuição de informações de nível "Confidencial".

g) Que permitam a transferência (*downloads*) de arquivos e/ou programas ilegais.

USO DO CORREIO ELETRÔNICO (*E-MAIL*)

O correio eletrônico fornecido pela GCS é um instrumento de comunicação interna e externa para a realização do negócio da GCS. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da GCS, não podem ser contrárias à legislação vigente e nem aos princípios éticos da GCS. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da GCS.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo. A utilização do "*e-mail*" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo. Não será permitido o uso de *e-mail* gratuitos (liberados em alguns sites da web), nos computadores da GCS, salvo quando autorizado. O Setor de Informática poderá, visando evitar a entrada de vírus na GCS, bloquear o recebimento de *e-mails* provenientes de sites gratuitos. A assinatura dos *e-mails* deverá seguir o padrão GCS e obrigatoriamente deverão ser utilizadas no primeiro *e-mail*.

NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da GCS em relação a definição de compra e substituição de "*software*" e "*hardware*". Qualquer necessidade de novos programas ("*softwares*") ou de novos equipamentos de informática (*hardware*) deverá ser discutida com o responsável pelo setor de Informática. Não é permitido a compra ou o desenvolvimento de "*softwares*" ou "*hardwares*" diretamente pelos usuários.

USO DE *LAP TOPS* (COMPUTADORES PESSOAIS)

Os usuários que tiverem direito ao uso de computadores pessoais (*laptop* ou *notebook*), ou qualquer outro equipamento computacional, de propriedade da GCS, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:

1. Fora do trabalho:
   a) Mantenha o equipamento sempre com você;
   b) Atenção em *hall* de hotéis, aeroportos, aviões, táxi e etc.
   c) Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
2. Atenção ao transportar o equipamento na rua.
3. Em caso de furto:
   a) Registre a ocorrência em uma delegacia de polícia;

b) Comunique ao seu superior imediato e ao Setor de Informática;
c) Envie uma cópia da ocorrência para o Setor de Informática.

REDES SOCIAIS

Todos os colaboradores são convidados a curtirem e acompanharem as nossas redes sociais, mas não acrescentar comentários que deva ser resolvido internamente na GCS. A área de marketing e comunicação é responsável pelos conteúdos e quaisquer necessidades de respostas. Não é permitido colaborador responder em nome da organização, salvo de autorizado, muito menos entrar em discussão, ainda que seja em defesa da organização.

IMAGENS DA ORGANIZAÇÃO

É proibido reproduzir imagens e sons de dentro da organização, sem uma prévia autorização, da área de TI que solicitará o conteúdo antecipadamente para uma breve avaliação.

RESPONSABILIADE DOS GERENTES / SUPERVISORES

A diretoria é responsável pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

a) Que tipo de informação o usuário pode acessar;
b) Quem está autorizado a acessar determinada rotina e/ou informação;
c) Quem acessou determinada rotina e informação;
d) Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
e) Quais informações ou rotinas, determinados usuários acessaram;

f) Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da GCS, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da GCS. Ao final de cada mês, se necessários, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa a GCS deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente *Internet* deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus é automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho. Os controles dos sistemas antivírus são mantidos pela GCS Global.

PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

HISTÓRICO DE REVISÕES

Data da Revisão	**Nº da Revisão**	**Histórico das Alterações**
22/03/2022	00	Emissão inicial aprovada.
08/04/2025	01	Revisão Geral