POLÍTICA DE SEGURANÇA DA INFORMAÇÃO GS3 TECNOLOGIA

1. OBJETIVO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos negócios da **GS3 TECNOLOGIA**.

2. ABRANGÊNCIA

Aplica-se a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento ou acesso as informações que pertençam a **GS3 TECNOLOGIA** e/ou a **SEUS CLIENTES**.

Qualquer usuário de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e garantir a integridade das informações e dos equipamentos tecnológicos.

3. CONCEITOS

A segurança da informação é caracterizada neste documento de acordo com os seguintes conceitos:

- **Confidencialidade**: Garante que a informação seja acessível somente pelas pessoas autorizadas;
- **Disponibilidade**: Garante que a informação esteja disponível para as pessoas autorizadas sempre que necessário;
- **Integridade**: Garante que a informação esteja completa e íntegra, que não tenha sido modificada, corrompida ou destruída de maneira não autorizada ou acidentalmente durante o seu ciclo de vida.

4. DEFINIÇÕES

Ativos de Informação: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.
Informação: resultado do processamento e organização dos dados (eletrônicos ou físicos) ou registros de um sistema.
Grupo Gestor da Segurança da Informação: grupo composto por administradores da **GS3 TECNOLOGIA** com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela empresa.
Segregação de funções: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que

nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.
Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida no desenvolvimento das atividades da GS3 TECNOLOGIA deve ser classificada de acordo com os níveis de confidencialidade a seguir:

1. **Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros devidamente autorizados. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao parceiro. **Exemplo:** propostas comerciais divulgadas indevidamente.
2. **Interna:** É toda informação que só deve ser acessada por colaboradores da organização. São informações com grau de confidencialidade que pode comprometer a imagem da empresa. **Exemplo:** atas de reuniões da diretoria.
3. **Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e/ou público em geral. **Por exemplo:** informações disponíveis na página da Internet da GS3 TECNOLOGIA ou Política de Privacidade e Dados Pessoais da GS3 TECNOLOGIA.
4. **Restrita:** É toda informação que pode ser acessada somente por usuários específicos 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. **Exemplo:** A folha de pagamento é de acesso restrito à apenas profissionais do setor de RH.

6. RESPONSABILIDADES

De forma global, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

- Cumprir fielmente a Política de Segurança da Informação da **GS3 TECNOLOGIA**;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades definidas pela **GS3 TECNOLOGIA**;
- Proteger as informações contra acessos, modificação, destruição ou divulgação indevidas;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual e proteção de dados;

- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais, sem expressa autorização da empresa;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.
- Considerar a informação como um ativo valioso da organização, um recurso crítico para a realização dos negócios, que portanto, deve ser tratada profissionalmente.

É de responsabilidade do Gerente/Supervisor de cada área classificar a informação (documentos, relatórios, procedimentos, modelos, e planilhas) gerada por sua área de acordo com o níveis de classificação da informação estabelecido neste documento.

São boas práticas que devem ser praticadas por TODOS:

- Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais trancados ou inacessíveis, quando não os estiver sendo utilizado.

7. DIRETRIZES GERAIS

A GS3 TECNOLOGIA 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 serão considerados confidenciais.

Os dados pessoais sob a responsabilidade da GS3 TECNOLOGIA não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados pessoais não serão transferidos para terceiros, exceto quando exigido em função do desenvolvimento do nosso negócio e, desde que, estes comprometa-se a manter a confidencialidade dos dados recebidos.

8. SOFTWARES ILEGAIS

É estritamente proibido o uso de programas ilegais (software pirata) na GS3 TECNOLOGIA. Os usuários não podem, em hipótese alguma, instalar este tipo de programa, aplicativo nos equipamentos da empresa, sob pena de responderem pelos danos causados em qualquer esfera.

Periodicamente, o Grupo Gestor da Segurança da Informação da GS3 TECNOLOGIA fará verificações nos servidores e/ou nos equipamentos dos usuários, visando garantir a correta aplicação desta diretriz.

9. ADMISSÃO E DEMISSÃO DE COLABORADORES

O setor de RH da GS3 TECNOLOGIA deverá informar ao Grupo Gestor da Segurança da Informação da GS3 TECNOLOGIA toda e qualquer movimentação de pessoal e/ou admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas específicos da empresa. O RH deverá objter junto ao setor demandante da contratação/demissão quais sistemas, pastas e equipamentos o novo colaborador deverá possuir direito de acesso.

O Grupo Gestor da Segurança da Informação da GS3 TECNOLOGIA fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo próprio usuário no seu primeiro acesso.

No caso de desligamento, o setor de RH deverá comunicar o fato na mesma data ao Grupo Gestor da Segurança da Informação para que os acessos concedidos sejam revogados.

Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos colaboradores em relação à Política de Segurança da Informação da GS3 TECNOLOGIA.

10. CONCESSÃO E REVOGAÇÃO DE ACESSOS

Quando houver necessidade de concessão ou revogação de acesso aos sistemas, repositórios de arquivos e/ou equipamentos de informática da GS3 TECNOLOGIA, o setor solicitante comunicará esta necessidade ao Grupo Gestor da Segurança da Informação da GS3 TECNOLOGIA.

11. POLÍTICA DE SENHAS

As senhas são individuais, sigilosas e intransferíveis, não podendo ser divulgadas em nenhuma hipótese. Resguardando o direito de propriedade empresarial.

As senhas devem ter no mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial.

Recomendamos que as senhas também sejam ser trocadas pelos usuários a cada 6 meses, não devendo repetir as senhas definidas nos últimos 12 meses.

Sempre que um usuário é desligado da organização, todas as suas senhas e acessos deverão ser, imediatamente, revogados.

12. ARQUIVOS DE TRABALHO

Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do negócio, são mantidos nos servidores de arquivos da GS3 TECNOLOGIA em sistema que permite o controle, comparação e gestão de diferentes versões, denominados Controladores de Versão, como por exemplo o ONEDRIVE, GIT, GITHUB e/ou SVN.

São exemplos de arquivos de trabalho:

- Planilha de faturamento;
- Notas fiscais;
- Propostas comerciais;
- Relatórios de análise técnica;
- Planilhas de medição;
- Documentação de sistema utilizada como insumo para o trabalho de análise e medição de software;
- Códigos de sistemas, rotinas ou procedimentos;
- E-mails dentre outros.

13. ARQUIVOS INDIVIDUAIS

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para clientes. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, instruções técnicas ou diagramas. A cópia de segurança destes arquivos é de responsabilidade exclusivas dos próprios usuários.

Não é permitido aos usuários o uso ou armazenamento dos seguintes tipos de arquivos em suas estações de trabalho:

- Programas não licenciados ou não homologados para uso na GS3 TECNOLOGIA;
- Músicas, filmes, séries, programas de TV;
- Vídeos não relacionados à atividade profissional;
- Jogos, apostas esportivas e similares;
- Conteúdo pornográfico ou relacionado a sexo;
- Conteúdos terroristas, descriminatórios, que estimulem uso de drogras ou qualquer conteúdo que ofenda as leis civis e penais do País.

14. COMPARTILHAMENTO DE DADOS

O compartilhamento de pastas e arquivos de trabalho cujo conteúdo seja classificado como sendo de informação **CONFIDENCIAL** ou **RESTRITA** é proibido através os seguintes :

- WhatsApp, Google Talk, Viber ou qualquer outro comunicador de mensagens instantâneas não homologados pela GS3 TECNOLOGIA;
- Compartilhamento de pastas do Windows;
- Bluetooth ou Airdrop;
- Cópia via pen drive ou qualquer outro dispositivo removível;
- Dropbox, Google Drive, iCloud ou qualquer outro drive virtual não homologado pela empresa.

15. CÓPIAS DE SEGURANÇA, RECUPERAÇÃO E INTEGRIDADE DOS SISTEMAS

Cópias de segurança dos sistemas, repositórios de arquivos de trabalho comuns, bancos de dados e configurações dos equipamentos e servidores de rede são de responsabilidade do Grupo Gestor da Segurança da Informação.

16. USO DA INTERNET

O uso da Internet é monitorado pela empresa por meio de sistema específico de registro de navegação que registra qual usuário está conectado, o tempo que usou a Internet e qual conteudo vizualizou.

A definição dos funcionários que terão permissão para uso (navegação) de sites restritos, como por exemplo, redes sociais, é atribuição da administração da empresa, a partir da solicitação de seu Gerente/Supervisor com a fundamentação da necessidade apropriada.

Os usuários devem assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- Estações de rádio;
- De jogos on-line;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a classes, raças ou etnias;
- Que promovam a participação em salas de discussão de assuntos relacionados aos negócios da GS3 TECNOLOGIA;
- Que não contenham informações que agreguem conhecimento profissional e/ou para o negócio da GS3 TECNOLOGIA

Qualquer acesso às redes sociais que não seja relacionado com a área de interesse da empresa não é permitido e, sendo assim, passível de punição.

17. USO DO CORREIO ELETRÔNICO

O correio eletrônico fornecido pela GS3 TECNOLOGIA é um instrumento de comunicação interna e externa para a realização dos negócios da empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da GS3 TECNOLOGIA, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos no "Código de Ética e Conduta – GS3 TECNOLOGIA".

O usuário do correio eletrônico é o unico responsável por toda mensagem enviada pelo seu endereço.

Não é permitido o cadastro de contatos pessoais nos sistemas de mensagens instantâneas (ao utilizar a conta profissional @gs3tecnologia.com.br); e nem a utilização de contas pessoais.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a "correntes", de conteúdos pornográficos, religiosos ou equivalentes;
- Possam prejudicar a imagem da GS3 TECNOLOGIA e/ou de outras empresas;
- Sejam incoerentes com as políticas e diretrizes estabelecidas no "Código de Ética e Conduta – GS3 TECNOLOGIA".

Não é permitido o uso de e-mail gratuitos (Gmail, Yahoo!, Hotmail, etc.), nos computadores da GS3 TECNOLOGIA.

O Grupo Gestor da Segurança da Informação poderá, visando evitar a entrada de vírus nos computadores da GS3 TECNOLOGIA, bloquear o recebimento de e-mails provenientes de e-mails gratuitos.

18. NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS

O Grupo Gestor da Segurança da Informação é responsável pela definição de compra, substituição e instalação de todo e qualquer "software" e "hardware".

Qualquer necessidade de novo “software” ou “hardware” deverá ser discutida com os responsáveis pelo Grupo Gestor da Segurança da Informação. Não é permitida a compra ou o desenvolvimento de “softwares” diretamente pelos usuários, sem aprovação do Grupo Gestor da Segurança da Informação.

19. USO DE EQUIPAMENTOS DA EMPRESA

Os usuários que estiverem de posse de qualquer equipamento (desktop, notebook, celular, tablet e etc) de propriedade da GS3 TECNOLOGIA devem estar cientes de que:

- Os recursos de tecnologia da informação disponibilizados, têm como objetivo a realização de atividades estritamente profissionais;
- A proteção e guarda 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, sob pena de arcar com as consequências de tal procedimento;
- O usuário não deve instalar ou remover nenhum programa do equipamento recebido sem prévia autorização do Grupo Gestor de Segurança da Informação. Também não deve alterar a configuração de nenhum programa previamente instalado.

Fora do escritório:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique o fato o mais rápido possível ao seu superior imediato e ao Grupo Gestor da Segurança da Informação;
- Envie uma cópia do boletim de ocorrência para o Grupo Gestor de Segurança da Informação.

20. RESPONSABILIDADES DOS GERENTES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da empresa, cabendo a eles verificarem se os mesmos estão acessando exclusivamente os sistemas e as áreas de dados 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 Grupo Gestor da Segurança da Informação fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinado sistema e/ou informação;
- Quem tentou acessar qualquer sistema ou informação sem estar autorizado.
- Quem acessou determinada sistema e informação;
- Que informação ou sistema determinado usuário acessou;
- Quem autorizou o usuário a ter permissão de acesso à determinado sistema ou informação;

21. SISTEMA DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos telefônes da GS3 TECNOLOGIA, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Grupo Gestor da Segurança da Informação, de acordo com as definições da administração da empresa.

22. USO DE ANTIVÍRUS

Todo arquivo obtido da Internet ou recebido de entidade externa a GS3 TECNOLOGIA deve ser verificado por programa antivírus.

Todas as estações de trabalho possuem software antivírus instalado. A sua atualização será automática, agendada pelo Grupo Gestor da Segurança da Informação, via rede.

O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

23. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

É qualquer ato que:

- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação

de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;

A violação dessa Política de Segurança ensejará ao violador as punições previstas na legislação civil e penal, além de reparação por eventuais perdas e danos a qual a empresa tenha sido submetida.

24. 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/serviços;
- outra ação disciplinar e/ou processo civil ou criminal.

25. VIGÊNCIA

O disposto no presente documento entrará em vigor na data de publicação do comunicado que o anunciar.

Li e consenti: