





GRUPO BSG

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O presente Código tem o objetivo de estabelecer e implementar a Política de Segurança da Informação (Dados e Tecnologia), além de determinar diretrizes com o objetivo de organizar, disciplinar, garantir a segurança e integridade dos dados e orientar as melhores opções, por ocasião das aquisições de equipamentos de informática.

1. DESCRIÇÃO

1.1. Condução da política de segurança de dados

A Gerência de Tecnologia da Informação é o usuário master dos sistemas de gestão do GRUPO, o qual se baseia em orientações e pareceres técnicos para conduzir a área de informática dentro dos padrões requeridos (incluídas as diretrizes ISO 27.001) para garantir o seu melhor aproveitamento, com a segurança necessária para os processos financeiros, contábeis, Recursos Humanos, Compras, etc.

1.2. Garantia da integridade dos dados

Para garantir a integridade, a continuidade e a qualidade dos dados do GRUPO, devem ser providenciados backup's diários dos servidores, onde serão armazenados todos os dados, não sendo permitido o armazenamento local de arquivos, além de promover a implementação de uma estrutura de proteção à invasão de vírus (firewall e antivírus corporativo).

1.3. Privacidade

É vedado a todo usuário qualquer acessibilidade às redes de comunicações externas que sejam incompatíveis com as atividades desenvolvidas pelas empresas do GRUPO, por exemplo, redes sociais.

A comunicação dos colaboradores deve ser realizada em um ambiente corporativo, por meio de um plataforma segura, evitando a entrada de vírus e acesso de hackers, o que pode ocasionar danos às informações empresariais.

1.4. Senhas individuais de utilização dos sistemas e perfil dos usuários

Implantação de senhas individuais para cada usuário utilizar os sistemas de gestão, além da criação dos perfis específicos dentro da necessidade de acesso às funções do sistema para

realização do trabalho, objetivando segurança na utilização dos sistemas de gestão.

1.5. Licenças de uso de software´s de gestão

A quantidade de licenças necessárias para o número de usuários será constantemente avaliada tecnicamente, dentro de uma política de compartilhamento de uso.

1.6. Instalação de software's fora do padrão e não licenciados

A empresa não permite que sejam instalados em seus equipamentos software's piratas ou fora do padrão estabelecido e a instalação de sistemas sem licenciamento (Windows, Office, antivírus, compactadores, sistemas de gestão, Autocad, Corel Draw), edvendo ser respeitado o número de licenças oficialmente adquiridas.

1.7. Utilização dos equipamentos de informática do GRUPO

Havendo a necessidade de retirada do equipamento das dependências do GRUPO, será necesária a aprovação pelo responsável.

Nesta hipótese, fica o colaborador responsável pelo seguinte:

- Efetuar o transporte do equipamento em local seguro e apropriado, para que não ocorram danos ao mesmo;
- Não deixar o equipamento dentro de veículos, estacionados em locais que possam levar na ocorrência de furtos;
- Cuidar para a utilização adequada do equipamento;
- Fica vedada a conexão física ou sem fio de celulares e tabletes diretamente no equipamento, para evitar a contaminação por vírus, etc.

1.8. Aquisição de equipamentos de informática e eletrônicos

Todas as necessidades de compras devem ser inicialmente requisitadas à área de compras/suprimentos da empresa. O equipamento solicitado será avaliado preliminarmente pela área de tecnologia.

1.9. Critérios de utilização de hardware's e software´s do GRUPO

Os hardware's e software's do GRUPO são de uso exclusivo e pessoal do colaborador designado para a utlização do equipamento e licenciamento do mesmo, não podendo ser objeto de

empréstimo ou cessão a terceiros.

1.10. Aplicação das melhores práticas para armazenamento e gravação de dados

Criação de uma estrutura capaz de armazenar todos os documentos e arquivos necessários para condução dos trabalhos de cada colaborador. Sendo vedado aos colaboradores armazenar arquivos de uso pessoal como filmes, música, etc., nos equipamentos do GRUPO.

1.11. Critérios e melhores práticas para garantir a segurança das informações

O colaborador deve ficar atento à recepção de e-mails suspeitos antes de abri-los procurando orientação com o setor de TI, bem como quanto ao uso de mídias externas fornecidas por terceiros (Pendriver's, Hds Externos e etc.)

Os equipamentos do grupo devem estar com bloqueio para conexão de mídias externas, e as autorizações de exceção devem ser feitas por escrito (e-mail) pela diretoria para o departamento de tecnologia.

Os colaboradores que tiverem permissão de acesso aos sites de bancos e compras, devem manter atenção na navegação, informando sempre ao setor de TI o que julgar fora de padrão. Tais usuários devem ter autorização escrita da Diretoria, informando o tipo de acesso liberado.

1.12. Política de restrição a divulgação de informações e dados do GRUPO

É vedado o compartilhamento de arquivos, hardware e dados das empresas do GRUPO com terceiros, além da publicação em redes sociais de documentos e opiniões pessoais a respeito do GRUPO.

1.13. Política de restrição e monitoramento de navegação na internet

A navegação na internet no ambiente corporativo do GRUPO é restrita e personalizada, tendo cada colaborador/departamento o acesso a determinados sites em conformidade com o tipo de trabalho realizado.

As permissões de acesso devem ser documentadas no Procedimento de Segurança de Informações, a fim de garantir o monitoramento adequado.

1.14. Diretrizes gerais de compliance e política de informática (política aplicada)

1.14.1. Os arquivos de uso corporativo de relevância para a empresa, serão salvos no servidor, não podendo ser salvos no disco rígido local da máquina ou em mídias

externas;

1.14.2. O servidor do GRUPO é adequado à rotina de backup;

1.14.3. Todo material impresso e não mais utilizado, deve ser destruído nos trituradores disponíveis, evitando-se, assim, a divulgaçao de informações restritas.

1.14.4. Eventual empresa contratada para administrar os servidores e infraestrutura, só poderá flexibilizar algumas das restrições das políticas apresentadas neste documento, mediante autorização da diretoria de operações.

1.14.5. Toda instalação de programa (sistema) deve ser restrita a softwares originais e adquiridos pelo GRUPO, e sua instalação somente poderá realizada por intermédio dos profissionais de suporte do setor de TI, sendo que isto não é permitido aos demais colaboradores;

1.14.6. É proibido a todos os colaboradores tirarem fotos de telas de computador, e de documentos de quaisquer das empresas do GRUPO;

1.14.7. É proibido disponibilizar o uso do computador das empresas a terceiros;

1.14.8. Nenhum equipamento de informática que não seja de propriedade das empresas do GRUPO poderá ser utilizado para exercício da função;

1.14.9. A rede WI-FI de visitantes poderá ser acessada por terceiros.

2. PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS

1.15. As informações confidenciais serão protegidas com o maior nível de rigidez possível.

1.16. As informações confidenciais devem ser compartilhadas apenas com as partes autorizadas.

1.17. É proibido divulgar dados de quaisquer pessoas físicas ou jurídicas que porventura se relacionem com o GRUPO BSG.

1.18. É proibido usar e divulgar informações confidenciais para outros fins que os comerciais legítimos.

1.19. As informações confidenciais devem, impreterivelmente, serem marcadas com indicações de como devem ser tratadas, distribuídas e destruídas.

1.20. As informações confidenciais não devem ser discutidas em ambientes em que outras pessoas possam tomar conhecimento do que está sendo dito, por exemplo: aviões, elevadores, restaurantes.

1.21. Documentos confidenciais devem motivar atenção redobrada dos seus portadores.

1.22. Os notebooks, dispositivos portáteis e mídias de armazenamento, que possam conter informações confidenciais ou proprietárias, devem ser mantidos em local seguro e seguir as políticas e protocolos de segurança da informação e da rede.

1.23. Qualquer violação potencial de segurança de dados deve ser informado ao gerente do setor ou ao diretor de operações.

2. RESPEITO A PRIVACIDADE E PROTEÇÃO DE INFORMAÇÕES PESSOAIS

2.14. A privacidade de todos os colaboradores e dos terceiros deve ser respeitada.

2.15. Os colaboradores devem ser transparentes sobre as práticas de privacidade do GRUPO BSG.

2.16. A Política de Tecnologia da Informação precisa ser plenamente cumprida para assegurar a proteção das informações pessoais dos colaboradores do GRUPO BSG.

2.17. O GRUPO BSG seguirá as disposições da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais), no que couber.

3. USO ADEQUADO DA TECNOLOGIA DA INFORMAÇÃO

3.14. A Política de Informática deve ser seguida para que o GRUPO BSG não seja exposto a riscos de violações de segurança, ações judiciais, sabotagem, vírus de computador ou problemas similares.

3.15. Os sistemas de Internet e os e-mails pertencem exclusivamente ao GRUPO BSG.

3.16. Em hipótese alguma, os sistemas poderão ser utilizados para enviar ou receber mensagens discriminatórias ou de assédio, correntes, material obsceno ou denatureza constrangedora, solicitações comerciais ou que, de qualquer modo, infrinjam a Política de Compliance.

3.17. Todas as mensagens enviadas ou recebidas por estes meios são de propriedade do GRUPO, cabendo a este, portanto, o direito de utilizá-las e divulgá-las em caso de litígio ou investigação judicial.

3.18. Os usuários e senhas eletrônicas de acesso à rede e outros sistemas do GRUPO BSG são pessoais, privativos e intransferíveis. As informações inseridas, geradas ou alteradas nos sistemas, assim como as aprovações realizadas são de responsabilidade exclusiva do usuário eletrônico que acessou o sistema.

3.19. É proibido divulgar ou ceder as senhas para outras pessoas, seja em caráter temporário ou permanente.

3.19.1. Todos os setores contarão com instruções de trabalho para melhor acesso e manuseio dos sistemas, com informações de suporte e de procedimentos de utilização padronizados.

4. CONSIDERAÇÕES FINAIS

4.1. Esta norma poderá ser alterada, diante de constada necessidade, ou por determinação da Ata Direção.