COPABO

POLÍTICA	Identificação: **PL03**	
	Revisão: **00**	Folha: **1 de 5**

Título:

SEGURANÇA DA INFORMAÇÃO - PSI

1. OBJETIVO

Esta Política tem o objetivo de estabelecer as diretrizes para a proteção das informações e da propriedade intelectual da 3BGP, orientando os colaboradores a seguirem padrões de comportamento que garantam a confidencialidade, integridade e disponibilidade das informações, bem como a proteção dos ativos de TI.

2. ABRANGÊNCIA

A presente Política abrange todos os colaboradores, incluindo: empregados, estagiários, diretores, sócios e acionistas, bem como os fornecedores e prestadores de serviços.

Todos os colaboradores devem cumprir as disposições dessa Política e assegurar que todos que tenham relacionamento com a 3BGP sejam informados sobre seu conteúdo.

3. DEFINIÇÕES

Para fins desta Política, alguns termos devem ser entendidos da seguinte forma:

- ***Ativos de TI****:* todos os componentes tecnológicos, físicos e virtuais da área de Tecnologia da Informação, tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação; podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas).
- ***Confidencialidade da Informação:*** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas e quando de fato for necessário.
- ***TI - Tecnologia da Informação:*** conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações do GRUPO 3BGP.

4. DIRETRIZES

As diretrizes que devem ser observadas e seguidas são:

4.1 ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Compete à Área de Tecnologia da Informação:
- Organizar, configurar os equipamentos, instalar e gerir os softwares e implementar os controles e auditorias necessários para **cumprir com os requerimentos de segurança desejados.**

- **Segregar as funções a fim de evitar conflito de interesse e autonomia excessiva do usuário**.

- **Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes** para a 3BGP.

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

- **Proteger continuamente todos os ativos de informação da 3BGP contra código malicioso** e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

- **Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da 3BGP** em processos de mudança.

- **Definir as regras formais para instalação de software e hardware** em ambiente de produção corporativo, exigindo o seu cumprimento.

- **Garantir que todos os softwares devem ser licenciados.**

- **Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários** (em ambientes internos e externos) por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da 3BGP.

- **Garantir a restauração dos servidores, mediante uso de plano de contingência**, conjunto este de medidas feitas para prevenir problemas e minimizar o impacto causado por uma falha.

- **Garantir atualização tecnológica de estrutura de rede wireless**, possibilitando isolamento de equipamentos estrangeiros (externos) da rede corporativa.

- **Definir em procedimento os detalhes operacionais da área.**

4.2 MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, a 3BGP poderá:

- **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.

- **Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade, bem como inspeções internas em caso de investigações a pedido do Comitê de Compliance ou da Diretoria Executiva.**

4.3 CORREIO ELETRÔNICO

- O uso do correio eletrônico da 3BGP é para **fins corporativos e relacionados às atividades do Colaborador usuário dentro da empresa.** A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a 3BGP e também não cause impacto no tráfego da rede.

- **É permitido à área de Tecnologia da Informação o acesso ao conteúdo de contas de e-mail alocados em arquivos .PST armazenados nas estações de trabalhos de todos os colaboradores.**

4.4 INTERNET

- **Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a 3BGP, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.**

- **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 Tecnologia da Informação.**

4.5 IDENTIFICAÇÃO E PERFIL DE USUÁRIO

- Todos os dispositivos de identificação utilizados na 3BGP, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos **têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais.**

- **Todo e qualquer dispositivo de identificação pessoal e senhas não podem ser compartilhados com outras pessoas em nenhuma hipótese.**

4.6 COMPUTADORES E RECURSOS TECNOLÓGICOS

- Os equipamentos disponíveis aos colaboradores são de propriedade da 3BGP, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, 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 Tecnologia da Informação da 3BGP ou de quem este determinar**.

4.7 DISPOSITIVOS MÓVEIS (notebooks, smartphones, tablets e de armazenamento externo)

- A 3BGP deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores e por isso, permite que eles usem equipamentos portáteis.

- A 3BGP, 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.

- O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na 3BGP, mesmo depois de terminado o vínculo contratual mantido com a instituição.

- **Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.**

- **O uso de dispositivos de armazenamento externo, tais como pen drives e discos rígidos é proibido e bloqueado, o mesmo somente poderá ser feito mediante requisição formal aprovada no sistema de chamadas pelo superior imediato e/ou Gestor de área.**

5. TREINAMENTO

A 3BGP, com o apoio do Comitê de Compliance, deve promover treinamentos periódicos aos colaboradores para disseminar as diretrizes do Código de Conduta e desta Política assegurando que os colaboradores realizem suas atividades de acordo com estas diretrizes.

6. COMUNICAÇÃO E DÚVIDAS

É de responsabilidade de todos os gestores da 3BGP divulgar para sua equipe o conteúdo desta Política e conscientizá-los sobre a necessidade e importância de sua observância e incentivá-los a apresentar dúvidas ou preocupações com relação a sua aplicação.

7. CANAL DE ÉTICA

Em caso de quaisquer atos, suspeitas de situações que violem esta Política, o Código de Conduta ou até mesmo em caso dúvidas, os colaboradores podem utilizar o Canal de Ética:

- ***E-mail:*** canaldeetica3bgp@iaudit.com.br
- ***Telefone:*** 0800 880 1865 (atendimento telefônico de segunda a sexta-feira, das 08h às 20h e, fora desse horário e feriados, via caixa postal)
- ***Internet:*** https://denuncia.iauditcloud.com.br/3bgp

Através do Canal de Ética, disponível 24 horas, é possível enviar relatos e denúncias de forma segura, sendo administrado por uma empresa especializada, garantindo ainda mais confidencialidade e segurança. Não é necessário se identificar quando usar o Canal de Ética, porém é fundamental agir com responsabilidade e embasar os relatos.

Não será permitida ou tolerada qualquer forma de retaliação contra as pessoas que realizam denúncias de boa-fé, conforme determina a Política de Realização de Tratamento de Denúncias.

8. SANÇÕES

O descumprimento por colaborador, fornecedor ou prestador de serviços de qualquer das disposições elencadas nesta Política e no Código de Conduta da 3BGP sujeitará os infratores às sanções:

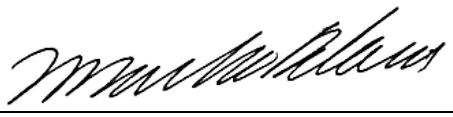
- Advertência;
- Suspensão;
- Demissão;
- Exclusão do fornecedor, prestador ou parceiro;
- Ação judicial cabível

9. HISTÓRICO DE REVISÃO

REVISÃO	DATA DA EMISSÃO	RESPONSÁVEL APROVAÇÃO	ALTERAÇÕES DA ULTIMA REVISÃO
01	26/05/2022	Fernando Borin Graziano Marcelo Borin Guedes Palaia	Revisão

10. APROVAÇÃO

Fernando Borin Graziano



Marcelo Borin Guedes Palaia