Política de Confidencialidade, Segurança da Informação e Segurança Cibernética

Sumário

1. Objetivo

Esta Política estabelece os princípios, diretrizes e controles de Confidencialidade e Segurança da Informação e Segurança Cibernética das Empresas BW. Seus processos foram estruturados para atender às exigências regulatórias aplicáveis, com abordagem baseada em riscos e alinhada ao apetite de risco definido pela Alta Administração e às melhores práticas de mercado.

Os controles aqui descritos foram aprovados pela Alta Administração, com orientação técnica das áreas de Segurança da Informação e de Compliance, visando assegurar a confidencialidade, integridade e disponibilidade das informações e a proteção do Ambiente Corporativo.

Esta Política deve ser lida em conjunto com:

- Código de Ética e Conduta Profissional;
- Política sobre Tratamento de Dados Pessoais (LGPD);
- Política Anticorrupção; e
- Política de Compras.

O Código e as Políticas estão publicados na Intranet das Empresas BW.

2. Aplicação da Política

Esta Política se aplica aos colaboradores das empresas (i) BW Gestão de Investimentos Ltda ("BWGI"), (ii) Brasil Warrant Administração de Bens e Empresas S.A. ("BWSA"), (iii) Brasil Warrant LLC ("BWLLC") e (iv) BW UK ("BWUK"), doravante "Empresas BW" e terceiros que prestem serviços as "Empresas BW" e que tenham acesso a Informações Confidenciais (conforme definido abaixo).

3. Terminologias e Definições

Seguem definições de termos utilizados no contexto desta Política:

- AMBIENTE CORPORATIVO: É o conjunto integrado de recursos tecnológicos, físicos e informacionais disponibilizados pelas Empresas BW para o desempenho das atividades profissionais de seus colaboradores e terceiros. Engloba, entre outros elementos, os Dispositivos Corporativos, os Sistemas Corporativos Homologados (conforme definidos nesta Política), ambientes físicos de trabalho, bem como os dados e informações corporativas acessados, processados ou armazenados durante a execução das funções.

- DADO PESSOAL: Informação relacionada a pessoa natural identificada ou identificável. Também são considerados Dados Pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural.

- DADO PESSOAL SENSÍVEL: Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculado a pessoa natural.

- DISPOSITIVOS CORPORATIVOS: São equipamentos de informática de propriedade das Empresas BW, fornecidos, homologados e gerenciados pelas áreas de Suporte, Infraestrutura de TI e Segurança da Informação, destinados ao acesso e uso dos Sistemas Corporativos Homologados, como por exemplo: *laptops* (*notebooks*) e estações de trabalho (*workstations* ou PCs). A Lista dos Sistemas Corporativos Homologados deve ser consultada junto ao time de Segurança da Informação. Para obter essa informação, o usuário deverá entrar em contato pelo e-mail: cybersecurity@bwgi.com.br

- DISPOSTIVOS PESSOAIS HOMOLOGADOS: São dispositivos de propriedade dos colaboradores e/ou terceiros, os quais são autorizados pelas áreas de Suporte, Infraestrutura de TI e Segurança da Informação das Empresas BW, destinados ao acesso e uso dos Sistemas Corporativos Homologados, como por exemplo: impressoras e celulares.

- INFORMAÇÕES CONFIDENCIAIS: são as informações proprietárias, que não são públicas, relativas às Empresas BW e aos seus respectivos negócios, incluindo, a título exemplificativo, mas não se limitando a:

  Informações Institucionais, Estratégicas e Operacionais

  - Estrutura organizacional, processos internos e modelo operacional;
  - Qualquer Dado Pessoal, sensível ou não, de clientes/acionistas e de colaboradores;
  - Estratégias e técnicas de negócio e planos / projeções de crescimento;
  - Situação financeira, demonstrações contábeis e análises de desempenho;
  - Histórico de investimentos, composição de portfólios, parâmetros de negociação e limites de risco;
  - Negociações estratégicas, contratos em andamento ou em fase de estruturação e lista restrita.

  Informações Técnicas e Tecnológicas

  - Sistemas, infraestrutura de tecnologia, *softwares* e ferramentas internas (em código-fonte ou objeto);
  - Modelos de análise, metodologias de avaliação, algoritmos e *engines* de precificação;
  - Estudos de negócio, mercado, que tenham sido desenvolvidos para as Empresas BW ou sejam de propriedade das Empresas BW.

- Políticas, procedimentos internos, metodologias de controle e gestão de risco;
- Ferramentas desenvolvidas ou contratadas para apoio à operação, análise ou conformidade regulatória;
- Projetos de inovação e soluções tecnológicas em curso.

Informações Comerciais e Contratuais

- Contrapartes, fornecedores, prestadores de serviço e seus respectivos contratos e condições comerciais;
- Acordos, termos de confidencialidade e estruturas de remuneração pactuadas com terceiros;
- Dados sobre pessoal interno, equipes, serviços corporativos e demais recursos humanos das empresas do grupo.

Informações sobre Investidores

- Identificação de cotistas e seus representantes legais;
- Informações patrimoniais, perfil de investimento, objetivos, necessidades e preferências;
- Dados Pessoais e Dados Pessoais Sensíveis, comerciais, produtos contratados, condições específicas, interações comerciais e quaisquer dados não públicos relacionados aos interesses dos cotistas.

- SISTEMAS CORPORATIVOS HOMOLOGADOS: Consideram-se Sistemas Corporativos Homologados todas as aplicações, ambientes tecnológicos, *softwares*, plataformas em nuvem, ferramentas digitais, soluções de telefonia, comunicação remota e redes de acesso, incluindo a rede Wi-Fi corporativa, cujo uso tenha sido previamente avaliado, aprovado e formalmente autorizado pelas Empresas BW, conforme os processos internos de homologação e critérios de segurança da informação. A Lista dos Sistemas Corporativos Homologados deve ser consultada junto ao time de Segurança da Informação. Para obter essa informação, o usuário deverá entrar em contato pelo e-mail: cybersecurity@bwgi.com.br .

4. Regras da Política

4.1) REGRAS PARA PROTEÇÃO DA INFORMAÇÃO

a) Princípios de Segurança da Informação

O compromisso das Empresas BW com o tratamento adequado das Informações está fundamentado nos seguintes princípios:

- Confidencialidade: garantir que o acesso à informação seja obtido somente

por pessoas autorizadas;

- Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

b) Uso de Informações Confidenciais

Durante a vigência do vínculo empregatício ou de prestação de serviços com as Empresas BW, os colaboradores e terceiros, poderão receber, acessar ou de qualquer forma obter Informações Confidenciais (definição constante no item 3 desta Política).

Todas as Informações Confidenciais são e permanecerão como propriedade única e exclusiva das Empresas BW, sendo reconhecido o legítimo interesse da organização na preservação e proteção de tais informações.

As Informações Confidenciais das Empresas BW devem constar e tramitar apenas em Sistemas Corporativos Homologados, os quais garantem a integridade e a salvaguarda da informação pelo tempo exigido pelas normas regulatórias, possibilitando rastreamentos e verificações.

É expressamente vedado ao colaborador e terceiro divulgar, compartilhar, utilizar ou permitir que outros divulguem ou utilizem quaisquer Informações Confidenciais para fins alheios aos interesses e às atividades das Empresas BW.

O colaborador e terceiro, comprometem-se a não remover Informações Confidenciais do Ambiente Corporativo das Empresas BW, exceto quando estritamente necessário para o desempenho de suas atribuições e desde que em conformidade com as Políticas e procedimentos internos vigentes.

Da mesma forma, é proibido copiar, reproduzir, transferir, baixar ou fornecer a terceiros, total ou parcialmente, por qualquer meio (inclusive eletrônico, como e-mail), Informações Confidenciais, salvo mediante autorização formal do Gestor da área e quando necessário ao exercício das atividades profissionais. Em caso de dúvida, consulte o Compliance.

É expressamente proibido utilizar Informações Confidenciais das Empresas BW para fins particulares.

As obrigações previstas nesta Política permanecerão válidas por prazo indeterminado, inclusive após o encerramento do vínculo empregatício e de prestação de serviços com as Empresas BW, independentemente da causa ou motivação da rescisão.

No momento da rescisão contratual, o colaborador e terceiro deverão cessar de forma imediata qualquer uso de Informações Confidenciais e de Produtos de Trabalho (incluindo, sem limitação, quaisquer aprimoramentos de materiais preexistentes), sendo vedada a utilização ou divulgação de tais informações ou produtos para qualquer finalidade, inclusive, mas não se limitando, a benefício de novo empregador ou nova

contratação de prestação de serviços.

c) Uso de Dados Pessoais e Dados Pessoais Sensíveis

As regras envolvendo Dados Pessoais e de Dados Pessoais Sensíveis (definição constante no item 3 desta Política) devem obedecer a Lei Geral de Proteção de Dados, cujas diretrizes constam na Política sobre Tratamento de Dados Pessoais.

As regras sobre incidentes de segurança de Dados Pessoais e Dados Pessoais Sensíveis constam do tópico 4.5.d desta Política.

d) Divulgação Obrigatória de Informações Confidenciais

Caso o colaborador ou o terceiro receba qualquer solicitação — judicial, administrativa ou de qualquer outra natureza — para divulgação obrigatória de Informações Confidenciais, deverá comunicar imediatamente a área de Compliance das Empresas BW, antes de qualquer divulgação, a fim de possibilitar que sejam adotadas medidas judiciais de proteção ou outras providências cabíveis.

O colaborador e terceiros devem cooperar com as Empresas BW para preservar a confidencialidade das informações, desde que tal cooperação não viole a lei ou decisões judiciais. Caso sejam legalmente obrigados a divulgar Informações Confidenciais e não haja medida judicial protetiva, a divulgação deve se limitar estritamente ao conteúdo exigido pela autoridade competente e com o apoio da área de Compliance.

As restrições previstas neste item não se aplicam nos seguintes casos:

- Quando a Informação Confidencial for revelada, de forma confidencial, a autoridade governamental competente (federal, estadual ou municipal), diretamente ou por meio de advogado, com o único propósito de relatar ou investigar uma suposta infração legal;
- Quando a Informação Confidencial for incluída em petição, queixa ou outro documento apresentado em processo judicial ou administrativo, desde que o protocolo tenha ocorrido sob sigilo judicial.

e) Devolução das Informações no Término do Contrato

No término do vínculo empregatício e de prestação de serviços com as Empresas BW, ou sempre que formalmente solicitado pelas Empresas BW, o colaborador e o terceiro deverão proceder com a devolução imediata de todas as Informações Confidenciais sob sua posse, independentemente do formato em que tais dados estejam armazenados (físico, digital, eletrônico, entre outros).

É vedado ao colaborador e aos terceiros apagar, modificar ou alterar qualquer informação armazenada em Dispositivos Corporativos fornecidos pelas Empresas BW antes da devolução desses dispositivos.

Na eventualidade do colaborador ou do terceiro ter utilizado equipamentos ou sistemas pessoais, (tais como computadores, dispositivos móveis ou outros meios de

armazenamento) para acessar, armazenar, revisar, preparar ou transmitir Informações Confidenciais das Empresas BW, deverá:

- Fornecer às empresas BW uma cópia utilizável em formato eletrônico (ou físico, se aplicável) de todo o conteúdo relacionado;
- Após o item anterior, realizar a exclusão definitiva e irreversível de todas as Informações Confidenciais desses dispositivos e sistemas pessoais. Sempre que possível, envolver a área de Tecnologia para apoio e acompanhamento da exclusão;
- Proceder com a destruição de quaisquer cópias físicas remanescentes.

Sempre que solicitado, o colaborador e terceiros deverão conceder às Empresas BW acesso aos sistemas ou dispositivos pessoais, eventualmente utilizados quando aprovados, com o objetivo exclusivo de verificar o cumprimento integral das obrigações de devolução, exclusão e destruição de Informações Confidenciais.

Segurança da Informação deve garantir que estas regras sejam cumpridas junto aos colaboradores e terceiros.

f) Conduta e Responsabilidade no Uso de Recursos Corporativos

Os colaboradores e terceiros, ao utilizarem os recursos disponibilizados pelas Empresas BW, ou seja, Dispositivos Corporativos e Sistemas Corporativos Homologados, no Ambiente Corporativo, representam institucionalmente as Empresas BW. Nessa condição, devem observar integralmente as diretrizes do Código de Ética e de Conduta Profissional, bem como as demais Políticas internas aplicáveis.

Esse princípio aplica-se a qualquer situação em que o uso de recursos da empresa possa associar a identidade do usuário as Empresas BW, inclusive quando utilizados para fins pessoais. Entre os recursos que caracterizam esse vínculo institucional, ou seja, do colaborador ou terceiro com as Empresas BW, destacam-se:

- ✓ Endereços de e-mail institucionais, vinculados ao domínio corporativo, utilizados para comunicações internas e externas;
- ✓ Dispositivos conectados à rede corporativa, incluindo o uso de Wi-Fi institucional;
- ✓ Dispositivos Corporativos, como por exemplo *notebooks*, operando sob endereçamento IP das Empesas BW.

É importante ressaltar que todo conteúdo armazenado ou trafegado no Ambiente e Dispositivos Corporativos pode ser acessado, monitorado e auditado a qualquer momento, inclusive as informações particulares dos colaboradores.

Dados Pessoais e Dados Pessoais Sensíveis que forem armazenados e processados legitimamente pelas Empresas BW serão tratados de acordo com as Leis de Proteção de Dados aplicáveis (exemplo LGPD).

Nesse contexto, colaboradores e terceiros devem estar cientes e concordar, por meio da assinatura do Termo desta Política, que as Empresas BW poderão, a qualquer tempo e sem aviso prévio:

- Acessar, armazenar e manter cópias de segurança (*backups*) de dados e comunicações trafegadas ou armazenadas em seu Ambiente Corporativo e em Sistemas Corporativos Homologados;
- Monitorar o conteúdo de mensagens, arquivos, sistemas e registros digitais, inclusive para fins de segurança, conformidade e investigação;
- Solicitar justificativas formais quanto ao uso de tais recursos, sempre que houver indícios de conduta inadequada, violação de Políticas ou uso indevido;
- Compartilhar registros e evidências com autoridades competentes, auditorias independentes ou assessorias jurídicas.

Caso o colaborador deseje transferir informações particulares armazenados em Dispositivos Corporativos para fora do Ambiente Corporativo das Empresas BW, deverá submeter solicitação formal ao seu superior hierárquico, que deve garantir que sejam realmente Dados Pessoais. Mediante aprovação, a área de Tecnologia da Informação realizará o procedimento de remoção segura, permitindo ao colaborador, se necessário, migrar previamente tais dados para seus dispositivos pessoais e, em seguida, eliminá-los do Ambiente Corporativo.

Caso o colaborador esteja em processo de desligamento, o prazo máximo para solicitar a transferência é de até 7 dias úteis, após este prazo, os Dados Pessoais poderão ser deletados.

g) Monitoramento de Comunicações / *Communication Surveillance*

A área de Compliance realiza um monitoramento das comunicações no Ambiente Corporativo com o objetivo de identificar potenciais indícios de abuso de mercado, condutas inadequadas ou riscos à integridade e reputação das Empresas BW, em conformidade com as leis e regulamentos aplicáveis, com o Código de Ética e de Conduta Profissional e com as Políticas internas.

Esse monitoramento pode incluir, mas não se limita à análise do conteúdo trocado por meio de contas de e-mail institucionais, Microsoft Teams, chats do Bloomberg (BBG) e outros Sistemas Corporativos Homologados. Todos os dados processados, armazenados ou transmitidos pelos sistemas das Empresas BW podem ser acessados, analisados e retidos pelas Empresas BW a qualquer tempo, sem aviso prévio e independentemente de seu uso ser profissional ou pessoal.

Os incidentes são analisados e endereçados, caso a caso pela área de Compliance, que dará privacidade a Dados Pessoais e os compartilhará com demais áreas, apenas em casos de legítimo interesse.

h) *Data Loss Prevention* (DLP)

Data Loss Prevention tem como objetivo evitar o vazamento de dados proprietários das Empresas BW para fora do Ambiente Corporativo.

Neste contexto, enfatizamos as seguintes disposições gerais de proteção de dados previstas nesta Política:

- Apenas Sistemas Corporativos Homologados podem ser utilizados no Ambiente Corporativo das Empresas BW (conforme definições constantes no item 3 desta política). É proibido aos colaboradores e prestadores de serviços o acesso ao Ambiente Corporativo por meio de dispositivos pessoais. Exceção ao uso de celulares particulares. As regras relacionadas ao uso de celular particular para acesso ao Ambiente Corporativo, encontram-se no item 4.2.c desta Política.
- É proibido modificar, instalar programas, ou alterar a configuração de Sistemas Corporativos Homologados sem autorização prévia da área de TI e Segurança da Informação
- É proibido aos colaboradores e prestadores de serviços enviar, compartilhar, copiar, transferir, por qualquer meio, permitir – de forma intencional ou não - que Informações das Empresas BW sejam enviadas para fora do Ambiente Corporativo das Empresas BW, salvo quando houver autorização formal do Gestor da área e finalidade legítima compatível com as atividades institucionais. Em caso de dúvida, consulte o Compliance.

Essa restrição aplica-se aos dados presentes no Ambiente Corporativo, especialmente às Informações Confidenciais, Dados Pessoais e Dados Pessoais Sensíveis, que não poderão ser transmitidos por qualquer meio fora do Ambiente Corporativo das Empresas BW, incluindo, mas não se limitando a:

- Contas de e-mail pessoal, assim como outros sistemas de mensagerias e chats não homologados;
- Plataformas de armazenamento em nuvem de uso pessoal;
- Mídias removíveis não autorizadas (como *pen drives* e HDs externos);
- Mídias Sociais; e
- Qualquer outro sistema não homologado, que permita *upload*, compartilhamento ou transmissão de dados para fora das Empresas BW.

Além das disposições gerais acima, aplicam-se, especificamente para a prevenção de vazamento de dados, as seguintes regras:

- Os colaboradores devem classificar, por meio da funcionalidade do Outlook (*Sensitivity > E-mail Confidencial – Criptografia*), todos os e-mails que contenham Informações Confidenciais e que sejam enviados para fora do Ambiente Corporativo das Empresas BW. Essa funcionalidade criptografa o e-mail e impede que seja encaminhado para destinatários que não os especificados

originalmente.

- A área de Segurança da Informação deve assegurar a existência de controles que impeçam o *upload* de informações para sistemas que não sejam homologados, bem como bloqueiem o acesso dos Dispositivos Corporativos a mídias removíveis.
- Será permitido o acesso a contas de e-mail pessoais a partir de Dispositivos Corporativos, porém com bloqueio da funcionalidade de upload de arquivos.
- É proibido o acesso ao WhatsApp Web e ao aplicativo WhatsApp e a mídias sociais por meio dos Dispositivos Corporativos, excetuando-se plataformas utilizadas para fins profissionais, como LinkedIn e X (Twitter).
- O monitoramento de DLP é um processo conduzido pela área de Segurança da Informação, com o objetivo de identificar situações passíveis de vazamento de dados e violações às regras desta Política e envolve as seguintes etapas:

- Mapeamento de dados: o time de Segurança da Informação se reúne com cada área das Empresas BW, para realizarem juntas, o mapeamento das informações que não podem vazar, e, portanto, devem ser monitoradas no processo de DLP.

    - A atualização dos mapeamentos, deve ser realizada anualmente e coordenada pelo time de Segurança da Informação junto as áreas.

    - Importante: As áreas são responsáveis por notificarem o time de Segurança da Informação (email: cibersecurity@bwgi.com.br) quando criarem e/ou identificarem novas informações que precisem ser monitoradas no processo de DLP.

- Definição de Modelos de Identificação: Com base no mapeamento, time de Segurança da Informação estabelece modelos para identificar se os dados monitorados estão sendo vazados do Ambiente Corporativo das Empresas BW.

- Implementação de sistema para identificar automaticamente incidentes passíveis de vazamento de dados, de acordo com os modelos de identificação estabelecidos.

- Análise de Alertas e Identificação de Incidentes: Quando o sistema de DLP identifica um possível vazamento, o alerta gerado é analisado pelo time de Segurança da Informação. Essa análise considera o conteúdo, o contexto do acesso e a intenção do usuário envolvido.

- Comunicação dos Incidentes e aplicação de ações disciplinares: Nos casos cuja análise indica um incidente real, o time de Segurança da Informação acionará o Colaborador e/ou terceiros responsável, copiando o gestor, Compliance e RH. Em caso de dúvida sobre o incidente, o time de Segurança da Informação deve acionar Compliance.

- *Key Risk Indicators* – KPI's: Segurança da Informação deve manter indicadores dos incidentes para reporte no Comitê de Compliance e Controles Internos, cuja periodicidade é trimestral.

- Revisão Contínua e Aprimoramento: a metodologia deve ser continuamente, no mínimo anualmente, revisada por Segurança da Informação, garantindo a adaptação a novas ameaças, mudanças de procedimentos internos, tecnológicos e regulatórios.

4.2) GESTÃO DE ACESSOS AO AMBIENTE CORPORATIVO

A concessão, revisão e revogação de acessos aos Dispositivos Corporativos e Sistemas Corporativos Homologados são realizadas exclusivamente por meio das ferramentas e processos definidos pelas Empresas BW, garantindo o controle e a rastreabilidade.

Todos os acessos devem ser individualizados e auditáveis, permitindo a identificação precisa do colaborador ou prestador de serviço que realizou o acesso ou alteração em informações, viabilizando a atribuição de responsabilidades.

Os gestores, que são responsáveis pelas permissões de acesso aos Sistemas Corporativos Homologados, devem observar o princípio do menor privilégio, devendo garantir que as permissões estejam estritamente alinhadas às responsabilidades funcionais do colaborador. Os gestores devem observar ainda, a segregação de funções, com o objetivo de evitar que uma mesma pessoa concentre as atividades de execução, controle e aprovação ao longo do ciclo de vida de um processo, fortalecendo os controles internos e reduzindo riscos operacionais.

O time de Segurança da Informação é responsável pela gestão dos acessos, sendo: Segurança da Informação como definidora das regras, TI como implementadora dos controles técnicos e Gestores das áreas como responsáveis pela aprovação contextual dos acessos.

a) Segurança dos Dispositivos Corporativos

O acesso ao Ambiente Corporativo é restrito a Dispositivos Corporativos, conforme definição constante no item 3 desta Política.

Não é permitido o acesso ao Ambiente Corporativo por meio de dispositivos pessoais. Exceção ao uso de celulares particulares, desde que atendam aos requisitos constantes no item 4.2.c desta Política.

O colaborador deve notificar imediatamente a área de Segurança da Informação (e-mail: cybersecurity@bwgi.com.br) em caso de perda ou roubo de Dispositivos Corporativos, suspeita de acesso não autorizado e qualquer incidente que possa comprometer a segurança da informação.

Os Dispositivos Corporativos devem ser configurados de acordo com os seguintes padrões mínimos de segurança:

- Soluções atualizadas de antivírus e *antimalware*;
- Políticas de senhas robustas e múltiplo fator de autenticação (MFA);
- Aplicação de patches e atualizações regulares;

- Bloqueio automático por inatividade;
- MDM (*Mobile Device Management*) para garantir a proteção, o gerenciamento e o monitoramento centralizado dos equipamentos que acessam Sistemas Corporativos Homologados e informações internas e confidenciais, conforme estabelecido nesta Política. Proporciona controle de acesso e limpeza remota.
- Auditoria e Monitoramento: Os Sistemas Corporativos Homologados poderão ser auditados para fins de segurança, conformidade com Políticas internas e investigações de incidentes.

b) Acesso Remoto

O acesso remoto ao Ambiente Corporativo das Empresas BW somente será permitido em condições que garantam a segurança da informação, a confidencialidade dos dados e a rastreabilidade das atividades realizadas.

O acesso remoto é permitido exclusivamente por meio de Dispositivos Corporativos, configurados com os padrões mínimos de segurança conforme estabelecidos nesta Políticas.

Todo acesso remoto à rede interna das Empresas BW deve ser realizado exclusivamente através das tecnologias fornecidos pela empresa, devidamente homologadas.

Para solicitar acesso remoto, os colaboradores devem solicitar autorização formal através do canal cybersecurity@bwgi.com.br.

c) Regras de Uso de Celular Pessoal (BYOD – Bring Your Own Device)

As Empresas BW permitem o uso de dispositivos pessoais (celulares) para acesso a determinados Sistemas Corporativos Homologados, desde que observadas integralmente as regras de segurança e conformidade aplicáveis.

O acesso ao Ambiente Corporativo por meio de celular particular está condicionado à adesão prévia às regras de segurança desta Política e à instalação das soluções de gerenciamento de aplicativos e dados corporativos (*Mobile Application Management* – MAM).

Enfatizamos, que o gerenciamento se restringe exclusivamente às aplicações e informações corporativas, não implicando acesso ou controle sobre Dados Pessoais armazenados no dispositivo, como imagens, arquivos, geolocalização, etc., conforme detalhamos a seguir.

Para tanto, o colaborador deverá, por meio da assinatura do Termo desta Política:

- Conceder autorização formal para adesão ao programa BYOD;

- Concordar com a instalação do aplicativo MAM (definição a seguir), fornecido pelo time de Segurança da Informação;
- Concordar com os termos de uso e consentimento de monitoramento de dados corporativos no dispositivo;
- Notificar imediatamente a time de Segurança da Informação em caso de perda ou roubo do dispositivo; suspeita de acesso não autorizado; qualquer incidente que possa comprometer a segurança da informação.

Mobile Application Management (MAM): As soluções de *Mobile Application Management* (MAM), também denominadas "container corporativo", têm como finalidade proteger o acesso e o uso de dados proprietários das Empresas BW em dispositivos móveis pessoais. Por meio do MAM, o acesso a e-mails, aplicativos de mensageria (como Microsoft Outlook e Microsoft Teams) e demais Sistemas Corporativos Homologados ocorre em um ambiente seguro e controlado, distinto do ambiente pessoal do usuário.

O MAM funciona pelo isolamento do Ambiente Corporativo dentro do container, assegurando que informações institucionais não possam ser copiadas, salvas, compartilhadas ou transferidas para fora desse espaço protegido. Dessa forma, as informações de propriedade das Empresas BW permanecem restritas ao ambiente seguro, sem interferência no uso pessoal do dispositivo.

Dentro do container, são aplicadas regras específicas de segurança, que incluem:

- Criptografia das informações;
- Bloqueio de compartilhamento de dados com aplicativos não corporativos;
- Restrição de abertura de *links* externos que direcionem o usuário para fora do ambiente das Empresas BW.
- Limpeza Remota (*Remote Wipe*): Consiste na exclusão remota de dados e Sistemas Corporativos Homologados apenas, armazenados no dispositivo, limitada a situações como perda, furto, comprometimento do equipamento, encerramento do vínculo com a empresa ou descumprimento desta Política.
- Auditoria e Monitoramento: Os aplicativos e ambientes corporativos poderão ser auditados e monitorados com o objetivo de garantir a segurança da informação, a conformidade com as Políticas internas e o suporte à investigação de incidentes.

As Empresas BW garantem que a gestão do dispositivo pessoal será estritamente limitada ao Ambiente Corporativo (container), não sendo possível acessar conteúdos pessoais; acessar a geolocalização do dispositivo; monitorar, alterar ou remover dados ou configurações pessoais do colaborador.

As Empresas BW garantem que a privacidade do colaborador será respeitada integralmente, nos termos da legislação vigente.

d) Acesso a informações e imagens

Todas as informações, dados, documentos, registros, imagens, conteúdos visuais, bem como quaisquer outros elementos produzidos, armazenados, processados ou transmitidos no Ambiente Corporativo, são considerados ativos institucionais de propriedade das Empresas BW, independentemente de sua forma, origem ou local de criação.

A solicitação formal para acesso interno as informações de *backups*, e-mails, inclusive em nuvem e imagens das câmeras de filmagem deve ser encaminhada a área de Compliance (email: compliance@bwgi.com.br) , com a justificativa e a autorizada pelo Gestor da área solicitante.

Compliance analisará a solicitação e se aprovada, encaminhará as ações necessárias aos responsáveis por conceder os acessos, com instruções, caso a caso.

e) Acesso por Terceiros ao Ambiente Corporativo

A contratação de terceiros, serviços ou sistemas de terceiros (como por exemplo, mas não se limitando a: plataformas de pagamentos, gestão de processos, gestão de dados, entre outros) os quais, no escopo de suas atividades, tenham ou possam vir a ter acesso ao Ambiente Corporativo e/ou Informações de propriedade das Empresas BW, principalmente as Informações Confidenciais, Dados Pessoais e Dados Pessoais Sensíveis, de acordo com a Lei Geral de Proteção de Dados (LGPD), devem ser previamente avaliados e aprovados pela área de Tecnologia da Informação, com posterior assinatura de Acordo de Confidencialidade, a ser validado pela área Jurídica.

Estes terceiros também devem aderir formalmente ao termo desta Política, comprometendo-se a agir de acordo com esta Política.

Detalhes dos procedimentos constam na Política de Compras.

4.3) SISTEMAS CORPORATIVOS HOMOLOGADOS

a) Aplicativos e Sistemas

Apenas Sistemas Corporativos Homologados (conforme definição constante no item 3 desta Política) podem ser utilizados no Ambiente Corporativo das Empresas BW.

Todas os sistemas homologados passam por análise técnica e possuem controles de segurança implementados, incluindo proteção contra vazamento de dados, controle de acesso, e aderência às normas internas de segurança da informação.

A instalação de qualquer aplicação ou *software* em Dispositivos Corporativos, ou conectados à rede da organização, deve ser previamente validada com a área de

Segurança da Informação, que poderá:

- Solicitar informações adicionais sobre a necessidade e o uso pretendido da aplicação;
- Submeter a solicitação à aprovação do gestor direto do colaborador requerente, quando aplicável;
- Rejeitar solicitações que não estejam em conformidade com os critérios estabelecidos que incluem, mas não se limitam a: segurança, finalidade de uso, licença válida, origem confiável do *software* e conformidade com Políticas internas.

b) Armazenamento e Processamento de Dados em Nuvem

Para fins desta Política, considera-se como "nuvem" qualquer serviço ou aplicação hospedada em infraestrutura de terceiros, acessível remotamente via Internet, *link* de dados, *link* de dados dedicado e qualquer outro meio de comunicação via IP, e que ofereça armazenamento, processamento ou gestão de dados corporativos.

Apenas aplicações em nuvem previamente homologadas pela área de Segurança da Informação estão autorizadas para uso pelos colaboradores.

As aplicações em nuvem aprovadas devem seguir os padrões mínimos exigidos de segurança, incluindo:

- Criptografia de dados em trânsito (especialmente para acessos via Internet pública);
- Criptografia de dados em repouso, quando aplicável;
- Controles de autenticação e autorização de acesso, preferencialmente com autenticação multifator;
- Conformidade com leis e regulamentos de proteção de dados (como LGPD, GDPR), especialmente quando o armazenamento ou processamento ocorre fora do território nacional.

Para aplicações que processam Dados Pessoais Sensíveis (LGPD), será exigido do responsável pela solução:

- Assinatura de cláusulas de confidencialidade e responsabilidade;
- Validação formal da existência e eficácia dos controles de segurança aplicados, conforme critérios definidos pela área de Segurança da Informação.

Caso não atendam aos padrões mínimos exigidos, o uso da aplicação poderá ser negado ou interrompido.

4.4) GESTÃO DE ATIVOS

As Empresas BW mantêm um controle rigoroso sobre todos os ativos utilizados em seu

Ambiente Corporativo. Isso inclui os Dispositivos Corporativos, os Sistemas Corporativos Homologados, instalações físicas e demais recursos que processam, armazenam ou acessam informações da organização.

Esta seção estabelece as regras para proteção, uso e controle desses ativos.

a) Identificação e Controle de Ativos

A área de Tecnologia da Informação (TI) é responsável por manter um inventário atualizado de todos os ativos tecnológicos da empresa.

Cada ativo possui um responsável designado, e deve ser registrado com informações como tipo, localização, finalidade e criticidade.

Colaboradores não devem instalar, conectar ou utilizar *softwares*, dispositivos ou sistemas que não tenham sido previamente autorizados e homologados pela área de TI e Segurança da Informação.

É proibido modificar, instalar programas, ou alterar a configuração de Sistemas Corporativos Homologados sem autorização prévia da área de TI e Segurança da Informação.

Caso o colaborador identifique qualquer uso indevido, falha de funcionamento, perda, roubo ou suspeita de comprometimento de um ativo, deve comunicar imediatamente a área de Segurança da Informação pelos canais oficiais.

b) Proteção Física e Lógica

A empresa adota controles físicos (como acesso restrito a salas técnicas, câmeras e biometria) e controles lógicos (como senhas, criptografia, antivírus, autenticação multifator e monitoramento) para proteger seus ativos contra acessos não autorizados.

Colaboradores devem zelar pela guarda e proteção de equipamentos sob sua responsabilidade, especialmente ao realizar atividades externas ou remotas.

A área de Facilities é responsável pelos controles de Proteção Física e Segurança da Informação pelos controles lógicos.

c) Monitoramento e Inventário

A área de TI realiza, periodicamente, verificações e auditorias nos ativos da empresa para garantir que estejam em conformidade com esta Política.

Durante essas verificações, podem ser identificados dispositivos não autorizados ou *softwares* fora do padrão — que serão bloqueados ou removidos.

O colaborador deve colaborar com esse processo, garantindo que seus Dispositivos Corporativos estejam disponíveis para inspeção quando solicitado.

d) Descarte Seguro

Colaboradores não devem descartar ou repassar equipamentos corporativos por conta própria. Qualquer devolução ou descarte deve ser conduzido junto à área de TI e Segurança da Informação.

O descarte de equipamentos, mídias e documentos que contenham informações da empresa consiste na eliminação de dados de forma que sua recuperação seja inviável, protegendo a confidencialidade, integridade e privacidade das informações corporativas, segundo os seguintes controles:

- Limpeza (*Clearing*): Exclusão lógica dos dados (ex.: formatação), dificultando o acesso casual.
- Sanitização (*Purging*): Aplicação de métodos que tornam a recuperação impraticável, mesmo com técnicas avançadas (ex.: sobrescrita com múltiplos padrões).
- Destruição Física: Fragmentação, incineração ou trituração de mídias (HDs, SSDs, DVDs, etc.), impossibilitando totalmente a recuperação.
- Registro do processo de descarte, com identificação da mídia, responsável e data.
- Uso de fornecedores certificados, quando o descarte for terceirizado.

4.5) SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

As Empresas BW adotam uma abordagem preventiva e estruturada para segurança cibernética, baseada na identificação de riscos, mitigação de vulnerabilidades e resposta tempestiva a incidentes.

a) Controles Mínimos

Os controles a seguir constituem o conjunto mínimo de práticas de segurança definidos pela área de Segurança da Informação das Empresas BW e são de aplicação obrigatória pela área de Tecnologia da Informação. Esses controles têm como finalidade proteger o ambiente corporativo contra ameaças cibernéticas internas e externas, assegurar a continuidade das operações e garantir a conformidade com os princípios de confidencialidade, integridade e disponibilidade da informação

- ✓ Gerenciamento de *Softwares* e Dispositivos: A instalação de *softwares* em Dispositivos Corporativos é de responsabilidade exclusiva da área de Tecnologia da Informação, sendo permitida apenas para aplicações previamente aprovadas pela área de Segurança da Informação das Empresas BW.

- ✓ Proteção de Dados e Ambientes Críticos: Os dados armazenados são protegidos por meio de soluções de *backup* seguras e mecanismos de criptografia, conforme diretrizes definidas pela área de Segurança da Informação e em alinhamento com a criticidade das informações. Os *backups* devem salvaguardar as informações conforme demanda

regulatória.

- ✓ Bancos de dados e dispositivos de rede são integrados a sistemas de segurança dedicados, com controles rigorosos de acesso e proteção, conforme diretrizes estabelecidas pela área de Segurança da Informação.

- ✓ Ambientes físicos críticos, como o Centro de Processamento de Dados (CPD), possuem controle de acesso físico e monitoramento por circuito fechado de televisão (CFTV), conforme os requisitos de segurança definidos pelas Empresas BW.

- ✓ Assinatura e Autenticação de Processos Críticos: O uso de assinaturas digitais é adotado nos processos classificados como críticos, devendo ser realizado por meio de soluções homologadas e controladas, garantindo a autenticidade, integridade e não repúdio das informações.

- ✓ Atualização e *Hardening* de Sistemas: Os sistemas operacionais e *softwares* utilizados pelas Empresas BW são mantidos atualizados por meio da aplicação regular de *patches* e correções de segurança, conforme definido pela área de Tecnologia da Informação e em alinhamento com as diretrizes da Segurança da Informação.

- ✓ Segurança Perimetral e de *Endpoint*: Implementação de *firewalls*, antivírus, filtros de *spam* e perfis restritivos para administradores de máquinas.

- ✓ Configuração segura e auditável dos serviços contratados em nuvem, com observância aos padrões de segurança exigidos pelas Empresas BW.

- ✓ Segurança no Desenvolvimento: As questões de segurança da informação são consideradas desde a fase de concepção de novos sistemas, *softwares* e aplicações, garantindo a adoção de práticas de desenvolvimento seguro, em conformidade com o princípio de *security by design.*

- ✓ Monitoramento e Resposta a Incidentes: Adoção de controles de auditoria, incluindo sistemas de gerenciamento de senhas, geração e análise de *logs* e trilhas de acesso. Monitoramento contínuo para detecção de ameaças, vulnerabilidades e comportamentos anômalos. Monitoramento das rotinas de *backup* e execução periódica de testes de recuperação de dados.

- ✓ Testes, Avaliações e Conscientização: Realização de avaliações periódicas de risco cibernético. Condução de testes de penetração (*pentests*) ao menos uma vez por ano, com análise de resultados e correção de falhas identificadas. Realização de simulações de *phishing*, acompanhadas de treinamento mandatório para os colaboradores envolvidos.

b) Avaliação de Riscos

A área de Segurança da Informação avalia os riscos e adota as medidas de segurança necessárias para proteger Dados Pessoais, Dados Pessoais Sensíveis e Informações

Confidenciais contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou vazamento.

A Gestão de Riscos inicia com uma avaliação de riscos e a implementação de controles baseados nos riscos, levando em consideração o ambiente de controle das Empresa BW, suas atividades, processos e clientes, bem como o mapeamento de Dados Pessoais e Informações Confidenciais.

A avaliação de riscos é atualizada periodicamente, com o objetivo de identificar novos riscos, ativos e processos que possam impactar a segurança da informação e a continuidade dos negócios.

A avaliação de riscos segue a metodologia do Risco Operacional, conforme respectiva Política.

A gestão de riscos contempla atividades de monitoramento contínuo e testes regulares, com o objetivo de detectar ameaças internas e externas e reforçar os controles de segurança. Inclui, ainda, a elaboração de um Plano de Resposta a Incidentes, que define previamente as ações de tratamento e recuperação, bem como o respectivo plano de comunicação.

c) Tratamento de Incidentes de Segurança da Informação

As Empresas BW adotam um processo estruturado para o tratamento de incidentes de segurança da informação e ataques cibernéticos, baseado em *frameworks* amplamente reconhecidos, como a ISO/IEC 27035, o NIST SP 800-61 e outras diretrizes de referência no mercado. Esse processo visa à identificação, contenção, mitigação, recuperação e aprendizado contínuo a partir dos eventos.

Incidentes de segurança da informação e ataques cibernéticos geralmente decorrem de vulnerabilidades técnicas, falhas humanas, acessos indevidos, uso de sistemas não autorizados ou violações de Políticas internas, podendo comprometer a confidencialidade, integridade e disponibilidade das informações corporativas.

Ataques cibernéticos são ações maliciosas com o objetivo de comprometer, interromper, danificar, acessar indevidamente, roubar ou manipular sistemas, redes, dispositivos ou informações digitais. Esses ataques exploram vulnerabilidades técnicas, falhas humanas ou fragilidades processuais para atingir seus objetivos, podendo causar prejuízos operacionais, financeiros, reputacionais e legais à organização. Os ataques cibernéticos mais comuns são:

- ✓ *Malware – softwares* desenvolvidos para corromper os computadores e redes, como: (i) Vírus: *software* que causa danos à máquina, rede, *softwares* e Banco de Dados; (ii) Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador; (iii) *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e (iv) *Ransomware*: *software* malicioso que bloqueia o acesso aos sistemas, arquivos e base de dados,

solicitando um resgate para que o acesso seja reestabelecido e as informações privadas não sejam expostas.

- ✓ Engenharia social – métodos de manipulação para obter Informações Confidenciais, como senhas, Dados Pessoais e número de cartão de crédito, como exemplo: (i) *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento; (ii) *Phishing*: anexos e *links* vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter Informações Confidenciais; (iv) *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter Informações Confidenciais; (v) *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter Informações Confidenciais; e (vi) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- ✓ Ataques de DDoS (*Distributed Denial of Services*) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.

- ✓ Invasões (*Advanced Persistent Threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico e ouros tipos de fraudes digitais.

Exemplos de incidentes de segurança da informação:

- ✓ Acesso não autorizado a informações ou sistemas;

- ✓ Perda, vazamento ou divulgação indevida de dados;

- ✓ Interrupções não planejadas em sistemas ou serviços críticos;

- ✓ Violação de Políticas internas de segurança ou de controles estabelecidos.

O colaborador tem o dever de comunicar qualquer suspeita, falha, violação ou comportamento anômalo que possa configurar um incidente a área de Segurança da Informação (e-mail: cybersecurity@bwgi.com.br).

Todos os incidentes de segurança da informação e de cibersegurança devem ser imediatamente reportados à área de Segurança da Informação (e-mail: cybersecurity@bwgi.com.br).

- ✓ A área de Segurança da Informação deve reportar ao Encarregado pelo Tratamento de Dados Pessoais (DPO) quando o incidente envolver Dados Pessoais (de acordo com a LGPD).

- ✓ A área de Segurança da Informação deve reportar o incidente como evento de Risco Operacional, conforme aplicável. Os eventos de Riscos Operacionais são apresentados no Comitê de Riscos, com periodicidade trimestral.

A área de Segurança da Informação é responsável por coordenar o tratamento dos incidentes, com apoio do SOC (*Security Operations Center*) 24x7 e demais áreas técnicas envolvidas, conforme item "Processo de Resposta a Incidentes" a seguir.

d) Tratamento de Incidentes de Segurança da Informação – Dados Pessoais

Caso um incidente de segurança envolva Dados Pessoais (LGPD) de qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de Dados Pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos Dados Pessoais, tem que ser comunicado a autoridade nacional e ao titular do dado. Para efetivar a comunicação o formulário disponibilizado no site da ANPD (Agência Nacional de Proteção de Dados) deve ser preenchido e enviado por meio do Sistema de Peticionamento Eletrônico.

A comunicação tem que ser feita o mais breve possível, considerando o prazo de 2 dias úteis, contados da data do conhecimento do incidente.

Nesses casos a ANPD (Agência Nacional de Proteção de Dados) aconselha:

- Avaliar internamente o incidente – natureza, categoria, quantidade de titulares de dados afetados, consequências concretas e prováveis;
- Comunicar o encarregado e o controlador;
- Comunicar a ANPD e o titular de dados (se considerado necessário);
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas.

O Encarregado de Proteção de Dados é responsável pela condução destes incidentes e a comunicação externa deve ser efetuada em conjunto com Compliance e Jurídico.

e) Monitoramento e Detecção

O Ambiente Corporativo das Empresas BW é continuamente monitorada por soluções que visam a identificar incidentes de segurança da informação e ataques cibernéticos, como:

- ✓ EDR (*Endpoint Detection and Response*): Solução instalada nos dispositivos finais (como *notebooks* e estações de trabalho) que realiza a detecção em tempo real de comportamentos suspeitos, análise de ameaças, contenção automatizada de incidentes, além de permitir resposta e investigação remota em caso de comprometimento;

- ✓ SIEM (*Security Information and Event Management*): Plataforma responsável por agregar, correlacionar e analisar eventos de segurança oriundos de diversos sistemas e dispositivos, gerando alertas em tempo real, identificando padrões de ataque e apoiando a tomada de decisão durante incidentes;

- ✓ Soluções de monitoramento de recursos e rede: Ferramentas que realizam o rastreamento contínuo do tráfego de rede, uso de recursos computacionais, acessos e serviços expostos, com alertas integrados ao SOC 24x7, que realiza a análise, triagem e resposta a eventos críticos em tempo integral;

- ✓ *Firewalls* corporativos: Dispositivos e soluções de segurança que atuam como barreiras de controle entre redes internas e externas, permitindo ou bloqueando tráfego com base em regras definidas. Os *firewalls* realizam a inspeção de pacotes, filtragem por portas e protocolos, prevenção contra conexões não autorizadas e contribuem para a segmentação e proteção da rede corporativa.

- ✓ Plataforma de *Threat Intelligence*: Sistema que coleta, analisa e correlaciona dados sobre ameaças cibernéticas, fornecendo informações acionáveis para identificar, prevenir e responder a ataques, apoiando a tomada de decisão em segurança da informação.

A detecção de incidentes de segurança da informação e ataques cibernéticos pode ocorrer por:

- ✓ Alertas automáticos gerados pelas ferramentas de segurança;

- ✓ Notificações de usuários ou de terceiros;

- ✓ Análises manuais ou periódicas de conformidade.

f) Plano de Resposta a Incidentes

O Plano de Resposta a incidentes segue as seguintes fases estruturadas, garantindo uma abordagem padronizada, eficiente e eficaz na contenção e resolução dos eventos.

- ✓ Identificação: Análise do evento, confirmação do incidente, classificação por severidade e impacto nos ativos, processos ou serviços da empresa.

- ✓ Contenção: Isolamento do incidente para evitar sua propagação, o que pode incluir o bloqueio de dispositivos, redes, contas de usuários ou conexões externas.

- ✓ Análise e Diagnóstico: Avaliação técnica do incidente, levantamento de danos, identificação da causa raiz e definição do plano de ação.

- ✓ Mitigação e Erradicação: Adoção das medidas corretivas e de contenção necessárias para erradicar o incidente, restaurando parcialmente os serviços, se necessário, até a resolução definitiva.

- ✓ Recuperação: Restauração segura dos sistemas, preferencialmente a partir de *backups* íntegros e verificados, garantindo o retorno ao estado operacional normal.

- ✓ Aprimoramento Contínuo: Registro das lições aprendidas, revisão dos controles falhos, atualizações em processos, ferramentas e treinamento de usuários, com base no ciclo PDCA (Planejar, Executar, Verificar e Agir). O registro, a rastreabilidade e a documentação dos incidentes são obrigatórias, e serão utilizados como base para auditorias, revisões de Políticas e ações preventivas.

Caso o incidente seja de vazamento de informações, a área de Segurança da informação enviará a comunicação ao usuário que cometeu o incidente, copiando o gestor, Compliance e Recursos Humanos.

Qualquer comunicação externa relacionada a incidentes de segurança da informação e cibersegurança deve ser coordenada exclusivamente pela área de Segurança da Informação, em conjunto com Compliance e Jurídico.

Em se tratando de incidentes relacionados a Dados Pessoais, o Encarregado de Proteção de Dados é responsável pela condução destes incidentes e a comunicação externa deve ser efetuada em conjunto com Compliance e Jurídico, conforme descrito no item 4.5.d desta Política.

Segurança da Informação deve manter indicadores (*Key Risk Indicators* – KPI's) dos incidentes para reporte no Comitê de Compliance e Controles Internos, cuja periodicidade é trimestral.

g) Plano de Contingência e Continuidade de negócio

Plano de contingência e de continuidade dos principais sistemas e serviços deverá ser implantado e testado periodicamente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

O Plano de Contingência e Continuidade de negócio está publicado em documento apartado desta Política, publicado na Intranet.

h) Testes Periódicos

A efetividade da Política de Segurança da Informação e Cibernética é verificada por meio de testes periódicos dos controles implementados, garantindo a identificação de falhas, oportunidades de melhoria e a conformidade contínua com os requisitos estabelecidos.

O plano de teste é efetuado pelo time de Segurança da Informação e proporciona avaliar:

- Que os recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação;
- Adequado nível de confidencialidade e acessos as Informações Confidenciais,
- segregação física e lógica;
- Que os recursos computacionais, de controle de acesso físico e lógico, estejam protegidos e
- Se a manutenção de registros permite a realização de auditorias e inspeções.

4.6) NORMAS DE CONDUTA DE SEGURANÇA

A segurança da informação é um compromisso coletivo. Todos os colaboradores, independentemente da área de atuação ou nível hierárquico, devem observar e cumprir as seguintes condutas obrigatórias de segurança em seu dia a dia, contribuindo ativamente para a proteção dos dados, sistemas e ativos informacionais das Empresas BW:

- Uso consciente do e-mail corporativo

  - ✓ Enviar mensagens apenas para os destinatários diretamente envolvidos no assunto, evitando a exposição desnecessária de informações. Redobrar a atenção ao incluir endereços externos, validando o domínio e o nome do destinatário.
  - ✓ Em caso de ausência programada (férias, licença ou viagens), configurar a mensagem de ausência temporária no Outlook, informando contato alternativo, se aplicável.
  - ✓ Mensagens de correio eletrônico que contenham Informações Confidenciais devem ser classificadas como “confidencial”. Para orientações sobre o procedimento correto de classificação, consultar a área de Segurança da Informação.

- Impressão e descarte de documentos

  - ✓ Imprimir apenas quando estritamente necessário, priorizando a redução do uso de papel e a proteção da informação.
  - ✓ Coletar imediatamente os documentos impressos.
  - ✓ O descarte de documentos que contenham Informações Confidenciais deve ser realizado de forma segura, por meio de lixeiras confidenciais ou procedimentos de fragmentação autorizados.

- Mensagens suspeitas e conteúdo inadequado

  - ✓ Diante de mensagens suspeitas, seja pelo título, conteúdo, anexo ou remetente, o colaborador deve evitar qualquer interação, como abrir, clicar ou responder. Nesses casos, a mensagem deve ser reportada imediatamente ao time de Segurança da Informação, utilizando o procedimento vigente, que deve ser validado junto à própria equipe de segurança.
  - ✓ Não repassar mensagens que contenham conteúdo indevido, duvidoso ou que violem as diretrizes da Política da BW. Em tais casos, comunicar imediatamente o time de Segurança da Informação.

- Proteção de Informações Confidenciais

- ✓ Informações Confidenciais, Dados Pessoais e Dados Pessoais Sensíveis seja em documentos físicos, telas de computador, anotações ou dispositivos eletrônicos devem ser mantidos sob vigilância e protegidos contra acesso ou visualização não autorizada, mesmo que temporária.
- ✓ Bloquear a estação de trabalho ao se ausentar da mesa.
- ✓ Utilizar senhas fortes, únicas e intransferíveis, mantendo-as em sigilo absoluto. Não as anotar nem as compartilhar com colegas ou terceiros.

- Postura preventiva e comunicação de incidentes

  - ✓ Atuar de forma diligente para identificar comportamentos de risco, falhas ou acessos indevidos.
  - ✓ Reportar imediatamente qualquer incidente, suspeita de violação de dados ou risco à segurança da informação ao time de Segurança da Informação, por meio dos canais internos designados.
  - ✓ Em caso de perda, roubo ou extravio de Dispositivos Corporativos, comunicar imediatamente a área responsável.

4.7) TERMO DE CONHECIMENTO

Os Colaboradores devem aderir formalmente ao termo desta Política, comprometendo-se a agir de acordo com as regras da mesma.

Terceiros, que tenham acesso a Informações Confidenciais e Dados Pessoais e Dados Pessoais Sensíveis, também devem aderir formalmente ao termo, comprometendo-se a agir de acordo com esta Política. Detalhes dos procedimentos constam na Política de Compras.

4.8) TREINAMENTO

Os colaboradores devem ser periodicamente treinados a respeito de Confidencialidade e Segurança da Informação e Segurança Cibernética.

Os temas constantes nesta Política são abordados no treinamento de *Onboarding*, efetuado pela área de Segurança da Informação, dentro do próprio mês no qual o colaborador é admitido nas Empresas BW. O referido treinamento tem o objetivo de conscientizar e capacitar os usuários quanto às melhores práticas e medidas de proteção, alinhados aos riscos e ameaças cibernéticas atuais, garantindo que todos estejam aptos a identificar, prevenir e responder a incidentes de segurança.

Trimestralmente, são conduzidas simulações de *phishing* para avaliar a efetividade dos treinamentos de segurança, o nível de conscientização dos usuários, identificar vulnerabilidades humanas e reforçar boas práticas de segurança no manuseio de e-mails e *links* suspeitos. Em caso de falha do usuário na simulação, o mesmo é direcionado para a realização de treinamento para reforço dos temas constantes no Treinamento de *Onboarding*.

4.9) PENALIDADES POR DESCUMPRIMENTO

O descumprimento das obrigações previstas nesta Política será passível de ações disciplinares, incluindo motivada rescisão do contrato de trabalho, bem como a responsabilização nas esferas cível e criminal, conforme a legislação aplicável.

5. Responsabilidades:

A BW instituiu e mantém um sistema de supervisão adequadamente estruturado para promover a conformidade com as leis e regulamentos aplicáveis. A responsabilidade pela implementação e manutenção de uma supervisão eficaz é atribuída aos Gestores e ao Compliance.

Esta Política deve ser aprovada pelo Diretor de Tecnologia da Informação, Diretor Jurídico e de Compliance e pelo Comitê Executivo.

Qualquer exceção às regras desta Política, devem ser submetidas a análise do Diretor de Tecnologia da Informação e do Diretor Jurídico e de Compliance, copiando o Comitê Executivo.

A Política deve ser revisada e aprovada, no mínimo, anualmente, ou após uma alteração material.

Mediante aprovação, o Responsável pela Política deverá comunicá-la da seguinte forma:

- Comunicação formal por e-mail a todas as partes interessadas relevantes.
- Publicação / disponibilização da Política na Intranet das Empresas BW, que é acessível a todas as partes interessadas.
- Publicar comunicado resumindo as alterações relevantes aos negócios / colaboradores impactados, sempre que houver modificações na Política.

Função	Responsabilidades
Colaborador	- Conhecer integralmente e cumprir todas as disposições desta Política. - Observar rigorosamente as regras de proteção da informação, incluindo o uso e a divulgação de Informações Confidenciais, Dados Pessoais e Dados Pessoais Sensíveis, bem como as normas de prevenção a vazamento de dados (DLP). - Cumprir as regras de conduta e responsabilidade no uso de recursos corporativos e dispositivos pessoais (BYOD), inclusive quando utilizados para fins particulares, estando ciente e de acordo com as condições previstas nesta Política.

	- Atender integralmente às normas de conduta de segurança estabelecidas. - Encaminhar dúvidas sobre a Política à área de Segurança da Informação e/ou ao Compliance. - Comunicar Segurança da Informação sobre perda ou roubo de Dispositivos Corporativos e celular particular, caso tenha acesso ao Ambiente Corporativo. - Informar a área de Segurança da Informação sempre que criar ou identificar nova informação que necessite monitoramento no âmbito do processo de DLP. - Em desligamento: devolver informações e dispositivos; excluir cópias pessoais após entrega à BW; solicitar transferência de dados pessoais próprios dentro do prazo. - Assinar o Termo de Conhecimento e participar de treinamentos. - Comunicar imediatamente ao Compliance qualquer violação à Política.
Gestores	- Comunicação e capacitação: assegurar que a equipe conheça e compreenda esta Política, com registro de treinamentos/aceites. - Supervisão e conformidade: monitorar a execução das atividades, corrigir desvios e manter evidências de cumprimento. - Gestão de acessos: solicitar, aprovar e revisar periodicamente (e revogar quando aplicável) as permissões nos Sistemas Corporativos Homologados, observando menor privilégio e segregação de funções. - Dados pessoais do colaborador: validar solicitações de exclusão/transferência de dados pessoais próprios em sistemas corporativos, conforme regras internas e com apoio de TI/SI/Compliance. - Compartilhamentos excepcionais: autorizar formalmente apenas quando estritamente necessários, com finalidade legítima, mínimo necessário, prazo/condições definidos, registro e, em caso de dúvida, consulta ao Compliance. - DLP e informações críticas: notificar Segurança da Informação sobre novas informações a monitorar e manter atualizado o mapeamento da área; responder a análises/alertas de DLP. - Auditorias e investigações: cooperar com auditorias internas/externas e fornecer evidências solicitadas. - Incidentes: comunicar prontamente incidentes à Segurança da Informação, acompanhar planos de ação e reforçar controles com a equipe. - Responsabilização: zelar pela aderência da área à Política e promover cultura de segurança.

Terceiros com acesso a sistemas, redes ou informação das Empresas BW	- Aderir formalmente a Política e cumprir integralmente as normas da mesma (procedimentos constantes na Política de Compras). - Guardar confidencialidade; usar apenas Ambiente/Sistemas Homologados; cumprir esta Política. - Assinar NDA (validado pelo Jurídico) e aderir formalmente ao Termo desta Política. - Ao término do contrato: devolver/excluir/destruir informações da BW; permitir verificação de cumprimento.
Segurança da Informação	- Garantir a devolução das informações ao término do contrato. - Implementar e manter os controles de DLP, gestão de acesso ao Ambiente Corporativo, gestão de ativos, Sistemas Corporativos Homologados, acesso remoto, MDM e MAM, monitoramento e processamento em nuvem, bem como demais controles relacionados à Segurança da Informação e Cibernética. - Manter listas atualizadas de Dispositivos Corporativos e de Sistemas Corporativos Homologados. - Manter controle de eventuais exceções às regras desta Política. - Tratar incidentes de Segurança da Informação e encaminhar ao Encarregado de Proteção de Dados aqueles que envolvam Dados Pessoais ou Dados Pessoais Sensíveis. - Coordenar a execução do Plano de Resposta a Incidentes. - Realizar testes periódicos dos controles de Segurança da Informação. - Comunicar casos de vazamento de informação ao usuário, copiando o gestor, Compliance e RH. - Reportar incidentes como eventos de Riscos Operacionais, quando aplicável. - Manter indicadores (KPIs) atualizados sobre incidentes, inclusive de vazamento de dados.
Compliance	- Responsável pelo procedimento de "*Communication Surveillance*", bem como pelo endereçamento dos incidentes. - Analisar e se aprovado, endereçar os pedidos de acesso a informações e imagens. - Trabalhar em conjunto com TI em incidentes de vazamento de dados. - Receber e decidir sobre pedidos de acesso interno a *backups*, e-mails e imagens de câmeras; acionar responsáveis. - Orientar e ser consultado em dúvidas sobre compartilhamento/divulgação; apoiar comunicações de incidentes e medidas disciplinares.

	- Participar de aprovações da Política e de exceções (com Diretores e Comitê Executivo); acompanhar KPIs no Comitê de Compliance e Controles Internos.
Encarregado de Proteção de Dados	- Conduzir incidentes com Dados Pessoais: avaliar risco, documentar medidas, e comunicar ANPD e titulares quando aplicável (prazo de referência: 2 dias úteis a partir do conhecimento do incidente). - Coordenar comunicações externas relativas a dados pessoais, junto com Compliance e Jurídico.
Facilities	- Controles físicos: acesso a áreas críticas (CPD), CFTV, barreiras e proteção de instalações. - Suporte a auditorias/investigações (fornecimento de registros físicos/câmeras mediante autorização de Compliance). - Colaboração com Segurança da Informação para alinhamento entre segurança física e lógica.

6. Contato:

Para maiores informações e/ou dúvidas, entrar em contato com o Responsável por Segurança da Informação e/ou Compliance.

Termo de Conhecimento da Política de Confidencialidade, Segurança da Informação e Segurança Cibernética

NOME		
ÁREA	*CARGO*	
DOC. IDENTIDADE Nº	*TIPO*	*CPF*

Declaro que tenho conhecimento da Política de Confidencialidade, Segurança da Informação e Segurança Cibernética e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) Adotar e cumprir as diretrizes indicadas na Política;
b) Comunicar imediatamente responsável por Compliance qualquer violação dessa Política que venha a tornar-se do meu conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação.

Declaro estar ciente de que o uso de meu celular particular para acesso ao Ambiente Corporativo das Empresas BW está condicionado ao cumprimento integral das respectivas regras da Política DLP, de forma que (i) autorizo a instalação do aplicativo de gerenciamento fornecido pela time de Segurança da Informação, (ii) concordo com os termos de uso e consentimento de monitoramento dos dados corporativos no meu dispositivo pessoal por meio desse aplicativo e (iii) notificarei imediatamente a time de Segurança da Informação em caso de perda ou roubo do meu dispositivo, suspeita de acesso não autorizado a ele, ou qualquer incidente que possa comprometer a segurança da informação das Empresas BW acessada por meio dele.

Declaro estar ciente de que todo conteúdo armazenado ou trafegado nos Dispositivos Corporativos e dependências das Empresas BW, ainda que sejam particulares, incluindo, mas não se limitando a acessos físicos, lógicos, voz e imagens, podem ser objeto de monitoramento, sem aviso prévio e sem garantia de privacidade e de *backup*.

Desde já, aceito incondicionalmente, sempre que solicitado, atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo termo, bem como em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____
(local)

_____
Assinatura do Colaborador