Política de Confidencialidade, Segurança da Informação e Cibernética

1. Objetivo:

A Política de Confidencialidade, Segurança da Informação e Cibernética ("Política") tem como objetivo estabelecer princípios e diretrizes envolvendo tecnologia, segurança da informação e segurança cibernética.

2. A quem se aplica a Política:

Esta Política é aplicável a todos os colaboradores das "empresas BW".

3. Regras da Política:

I - DEFINIÇÕES

I.1. Informações Confidenciais: são consideradas informações confidenciais aquelas, não disponíveis ao público, que:

- identifiquem dados pessoais ou patrimoniais.
- clientes e suas operações.
- sejam objeto de acordo de confidencialidade celebrado com terceiros.
- identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva.
- o colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.

Não se caracteriza descumprimento desta Política a divulgação de informações confidenciais quando em atendimento a determinações decorrentes do Poder Judiciário ou Legislativo, de órgãos fiscalizadores e reguladores. Ou quando a divulgação se justificar, por força da natureza do negócio, a advogados, auditores e contrapartes.

I.2. Ataques cibernéticos / Cibersegurança: Os ataques cibernéticos mais comuns são:

- Malware – softwares desenvolvidos para corromper os computadores e redes, como: Vírus: software que causa danos à máquina, rede, softwares e Banco de Dados; Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador; Spyware: software malicioso para coletar e monitorar o uso de informações; e 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: Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; Phishing: anexos e links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e 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.

II - DISPOSIÇÕES GERAIS

Os seguintes princípios norteiam a segurança da informação:

- Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas e quando ele for de fato necessário;
- Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
- Integridade: a informação deve ser mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os colaboradores:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida.

- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns, quando aplicável.
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.
- Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao responsável pelo Compliance.

Para que os recursos disponibilizados pela BW sejam utilizados da maneira correta e segura, atentar para as boas práticas listadas abaixo:

- Enviar mensagens curtas e objetivas, colocando identificação clara e precisa do assunto.
- Somente enviar mensagens para as pessoas envolvidas no assunto a ser tratado e certificar-se dos endereços de destino escolhidos.
- Somente imprimir as mensagens quando forem realmente necessárias.
- Ao identificar mensagem com título ou anexo suspeito, certificar-se com a Tecnologia da Informação, se existe problema em abri-la. Ela pode conter um vírus ou código malicioso.
- Caso receba mensagens que contrariem as regras estabelecidas pela BW, nunca as repasse e alerte Tecnologia da Informação.
- Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloqueie a estação de trabalho.
- Quando sair de férias ou se ausentar por períodos prolongados, utilize o recurso de ausência temporária do Outlook.

III - PROCESSOS E CONTROLES

Controles de Segurança da Informação Confidencial.

Para assegurar que as informações confidenciais sejam adequadamente protegidas, as Empresas “BW” definiram os seguintes processos / controles:

III.1. Identificação da Informação

O colaborador que recebe ou prepara uma informação é responsável por identificar a natureza desta, conforme o item a seguir.

III.2. Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Restrita e Pública.

- Informação confidencial: definida conforme item I.1.
- Informação restrita: a informação que poderá ser acessada por um grupo específico de pessoas, justificada a sua necessidade.
- Informação pública: informação que já é divulgada ao público em geral e que portanto, se divulgada por necessidade de negócio, não provocará impactos.

Para a classificação devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

III.3 Controles para informações classificadas como "Confidencial"

Informações confidenciais devem ser identificadas como tal: e-mails, apresentações, documentos.

Os e-mails e arquivos com informações confidenciais devem ser protegidos.

O acesso às informações confidenciais deve ser controlado.

Qualquer documento pessoal que seja disponibilizado a terceiros devem ser enviado com a identificação do terceiro, editada em marca d'água.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

III.4. Controles de Segurança da Informação e Cibernética

Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento e Descarte.

O colaborador, responsável pela informação gerada, deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte.

Na dúvida do tempo regulatório, questionar o Jurídico.

O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Gestão de Acessos

Controles de Gestão de Acessos, que devem ser garantidos por Tecnologia da Informação:

- Controle de acesso envolvendo identificação, autenticação e autorização dos usuários.
- Definição de regras para senhas de acesso aos sistemas corporativos, prevendo inclusive a troca periódica das mesmas.
- Definição de perfil de acesso aos sistemas internos e externos de colaboradores, terceirizados e prestadores de serviços, principalmente às informações confidenciais.
- Controle dos acessos de colaboradores, terceirizados e prestadores de serviços em caso de desligamento e encerramento das atividades.
- Os acessos físicos e do ambiente corporativo, inclusive por meio remoto e por meio de dispositivos pessoais como celulares, devem ser rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria e possam identificar individualmente o Colaborador, para que o mesmo seja responsabilizado por suas ações.
- Homologação dos equipamentos, ferramentas e sistemas concedidos aos colaboradores e configuração com os controles necessários para cumprir os requerimentos de segurança aplicáveis às “Empresas BW”.

Controles de Segurança Física e controles de acesso às instalações, que devem ser garantidos pela área Administrativa:

- Controle de acesso por meio de crachás e filmagens.
- Espaço físico adequado e restrição de acesso para a guarda de equipamentos e informações confidenciais.

Utilização e monitoramento dos equipamentos e serviços eletrônicos

É permitido o uso dos equipamentos e recursos como internet, inclusive rede wi-fi, e-mails, sistemas, computadores, telefones e gravação de voz pertencentes às Empresas "BW" para fins particulares, com moderação, respeitando princípios éticos e de integridade.

Estes dispositivos são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria e/ou exigência judicial.

Importante ressaltar que nesses casos, o colaborador é identificado como vinculado às "Empresas BW" seja pelo e-mail corporativo ou pelo Internal Protocol (IP) e, portanto, deve seguir os mesmos padrões definidos no Código de Ética e Conduta Profissional, estar ciente e concordar que as "Empresas BW" poderão:

- Acessar e manter back up de informações particulares, ainda que criptografadas.
- Monitorar seu conteúdo.
- Solicitar justificativa pelo uso, caso necessário.
- Disponibilizar os recursos a terceiros, quando aplicável, como por exemplo em auditorias e fiscalizações.

O monitoramento é efetuado pelo Compliance.

Acesso interno a informações

A solicitação formal para acesso interno a informações de backups, e-mails, inclusive em nuvem e gravações telefônicas deve ser encaminhada a área de Tecnologia da Informação com a justificativa e a autorização do responsável da área do solicitante e a do Compliance.

Apenas o administrador de Tecnologia da Informação tem acesso as informações e será o responsável por garantir o cumprimento desta regra.

Bloqueios de Acessos

A Segurança da Informação é responsável por administrar e monitorar os acessos a sites a partir da BW, com o objetivo de verificar o mau uso dos recursos para reporte à gestão e bloquear o acesso a sites proibidos.

As "Empresas BW" devem, via de regra, bloquear os acessos a dispositivos móveis, como pen drive, hd externo, celular, cartão de memória.

Exceções devem ser aprovadas pelo Responsável por Compliance.

Sites de armazenamentos de arquivos

O acesso a sites de armazenamento de arquivos em "nuvem" é permitido somente nas plataformas AWS, One Drive for Business e Evernotes, todos mantidos pela BW.

Exceções devem ser aprovadas pelo Responsável por Compliance.

Segurança Cibernética

Controles de Segurança Cibernética, que devem ser garantidos por Tecnologia da Informação:

- Apenas a área de Tecnologia da Informação autoriza e/ou realiza o download e instalação de softwares.
- Proteção dos dados armazenados, contendo ferramenta segura de backup e criptografia, conforme necessário; bancos de dados e dispositivos de rede devem ser enviados para um sistema de segurança dedicado que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;
- Uso de assinaturas digitais para alguns processos/colaboradores críticos;
- Atualização dos sistemas operacionais e softwares utilizados na instituição;
- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores das máquinas, filtros de spam, controle para uso de periféricos (pendrives, CDs e HDs);
- Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;
- Realização de avaliações periódicas de risco cibernético.
- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acesso;
- Controle de acesso e CFTV no ambiente do CPD.
- Contrato de manutenção com Suporte 24x7 dos Servidores.
- Configuração dos serviços contratados em nuvem.
- Monitoramento e testes para detecção de ameaças.
- Monitoramento das rotinas de backup e testes para recuperação dos dados.
- Realização de teste de penetração.
- Controle de rastreamento do e-mail corporativo nos dispositivos móveis dos colaboradores.

Gestão de Riscos

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 da Empresa, suas atividades, processos e clientes. A avaliação de riscos deve ser atualizada de forma a identificar novos riscos, ativos e processos.

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

A gestão de Riscos deve contemplar monitoramento e testes com o objetivo de detectar as ameaças e reforçar os controles, bem como criação de Plano de Resposta que é o planejamento prévio para tratamento e recuperação de incidentes, incluindo um plano de comunicação.

Tratamento de Incidentes de Segurança da Informação / Plano de Resposta,

Qualquer evento que envolva segurança da informação e segurança cibernética deve, imediatamente, ser reportado ao responsável por TI.

O responsável por TI aciona a empresa de segurança da informação que segue os 5 passos da metodologia de resposta à incidentes.

- Identificação e Classificação – Uma vez informados pela equipe interna do cliente o time de resposta à incidentes da Morphus irá atuar na classificação do incidente. Para isso a equipe pode basear-se em notificações externas ou em um conjunto de ferramentas de monitoração. Os esforços da equipe concentram-se em identificar os sintomas do ataque e suas características, observando a severidade do incidente, ou seja, o quanto a estrutura de negócios da instituição afetada.
- Contenção – Isolar os sistemas impactados de imediato para evitar que outros dispositivos sejam contaminados, implementando bloqueio em nível de rede, como isolar a tráfego de um computador ou até mesmo de uma área, em casos mais graves considerar desligar temporariamente conexões com a internet, preservando o estado da memória para avaliação futura. Identificar possíveis usuários ofensores e realizar o bloqueio ou desativação temporário.
- Coordenação – Após identificar a existência de um incidente e suas consequências na etapa anterior a equipe identificará os danos causados pelo incidente em questão. A avaliação dos sintomas coletados permitirá diagnosticar de forma preliminar a causa do problema, ou pelo menos inferir algumas conclusões que serão úteis para determinar o plano de ação a ser colocado em prática.
- Mitigação – Isolar o problema e determinar a extensão dos danos através da execução do plano de ação delineado na etapa anterior. Além de utilizar procedimentos para isolar o incidente evitando a propagação do ataque, a equipe atuará em pró de restabelecer o serviço, que porventura tenha sido comprometido, mesmo que seja com uma solução temporária, até que a solução definitiva seja encontrada e posteriormente adotada.
- Investigação e erradicação – A equipe atuará na coleta e análise as evidências do incidente. O processamento de evidências como registros, arquivos de pacotes capturados e até mesmo entrevistas com os

responsáveis são muito importantes para eleminar o problema em sua totalidade e na resolução de futuros incidentes com características semelhantes.

- Plano de recuperação – Uma vez que o problema foi erradicado e temos certeza que todo o ambiente esta integro devemos restaurar os sistemas se possível por backups íntegros ou em situações extremas refazer toda a estrutura do início.
- Aprimoramento – Esta etapa consiste em avaliar o processo de tratamento de incidentes e verificar a eficácia das ações adotadas. As lições aprendidas durante todo o processo serão catalogadas e propagadas com base no PDCA.

Os riscos e incidentes de Segurança da Informação devem ser reportados ao Responsável pelo Compliance, que analisará caso a caso e adotará as medidas cabíveis, bem como reporte ao Comitê de Riscos, Compliance e Controles Internos e compartilhamento de informações, se aplicável.

Caso um incidente de segurança envolva dados pessoais 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, teremos que comunicar a autoridade nacional e ao titular a ocorrência do incidente de segurança que possa acarretar risco ao dano relevantes aos titulares, para efetivar a comunicação devemos responder o formulário disponibilizado no site da ANPD (Agencia Nacional de Proteção de Dados) e enviá-lo por meio do Sistema de Peticionamento Eletrônico.

Antes de notificar a autoridade nacional devemos efetuar uma avaliação interna de relevância do risco ou dano do incidente, confirmado temos o comunicado o mais breve possível, considerando o prazo de 2 dias úteis, contados da data do conhecimento do incidente.

Nesses casos a ANPD (Agencia 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 (Art. 6º, X da LGPD).

Backups, Plano de Contingência e Continuidade de negócio

Plano de contingência e de continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Os mesmos controles de segurança e controle de acesso devem ser aplicáveis nas instalações do site de contingência.

Deve haver backup e que os mesmos sejam testados anualmente.

Testes de Controles

A efetividade da política de Confidencialidade, Segurança da Informação e Cibernética deve ser verificada por meio de testes periódicos dos controles existentes.

O plano de teste é efetuado pelo responsável por Tecnologia da Informação assegurando que:

- 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. As informações confidenciais são definidas pelo DPO da BW.
- recursos computacionais, de controle de acesso físico e lógico, estejam protegidos,
- manutenção de registros que permita a realização de auditorias e inspeções.

IV. Propriedade Intelectual

Tecnologias, marcas, metodologias, produtos, técnicas e quaisquer informações que pertençam as Empresas “BW” não devem ser utilizadas para fins particulares, nem repassadas a outrem. Aquelas desenvolvidas pelo próprio Colaborador no exercício das suas atividades nas Empresas BW são de propriedade das mesmas.

V. Termo de Conhecimento

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com a política de Segurança da Informação.

Terceiros, que tenham acesso a informações confidenciais também devem aderir formalmente ao termo, comprometendo-se a agir de acordo com a política de Segurança da Informação.

Compliance é responsável por manter controle dos termos e salvaguarda dos mesmos.

VI. Treinamento

Os colaboradores que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento devem ser treinados a respeito de Segurança da Informação e Cibersegurança.

4. Responsabilidades:

Os assuntos de Segurança são tratados no Grupo Técnico de Segurança da Informação, com representantes das áreas de Tecnologia, Infraestrutura e Compliance e os assuntos relevantes sobre o tema são reportados no Comitê de Compliance e Controles Internos.

Compliance é indicado como ponto de contato para assuntos deste tema para o regulador e ANBIMA.

Os colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao responsável por Compliance, a quem caberá avaliar e submetê-las ao Conselho de Ética, que tomará as medidas cabíveis.

O responsável por Tecnologia da Informação é responsável pela implementação dos procedimentos e controles técnicos inerentes a esta Política, bem como pelos testes de controle, podendo ser realizados por terceiros, independentes.

5. Contato:

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

Termo de Conhecimento da Política de CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

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

Declaro que tenho conhecimento da Política de CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO 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.

Estou ciente de que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

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